Groningen Journal of International Law

VOLUME 2 / ISSUE 2 / 2014

Privacy in International Law: Regulating the Internet

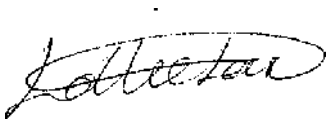
Dear Readers,

I am extremely happy to be writing the Editorial Note for vol. 2 ed. 2 of the Groningen Journal of International Law: Privacy in International Law: Regulating the Internet. The topic of this issue has been at the forefront of recent discussions on international regulation, and poses many challenges to both regulatory systems and scholars alike.

Major scandals, such as those surrounding the NSA, and worries over the privacy terms and conditions of various social media networks have raised questions regarding the ability of individuals to protect their privacy online. This has become a huge concern across the globe. One of the main issues faced is how to protect users' privacy through regulation of the Internet. This is not an easy feat; vast and continuous developments in technology, including the "Internet of Things", make it extremely demanding to address this transnational issue effectively. In this issue of GroJIL, the contributions tackle different aspects of the multifaceted problem, making suggestions as to how international law can deal with the fast-paced challenges.

I am very proud to be publishing this issue of GroJIL, into which the Journal's participants have put an enormous amount of work. I could not be more grateful to the fantastic Editorial Board, with whom it has been an absolute pleasure to work. The Board has worked closely together to develop GroJIL's editing process, internal workings, and the Board's dedication and drive to move GroJIL forwards has resulted in the most successful and rounded issue of the Journal to date. In addition to the Board, both new and old members of the Editing Committee and Events Committee have done a tremendous job in editing this issue's articles. I would like to take the opportunity to thank all of our members for their continuous commitment to the Journal, and I look forward to working with them again on our next issue dealing with international arbitration.

Happy reading!



Lottie Lane
President and Editor-in-Chief
Groningen Journal of International Law

Groningen Journal of International Law

Crafting Horizons

ABOUT

The Groningen Journal of International Law (GroJIL) is a Dutch foundation (Stichting), founded in 2012. The Journal is a not-for-profit, open-access, electronic publication. GroJIL is run entirely by students at the University of Groningen, the Netherlands, with supervision conducted by an Advisory Board of academics. The Journal is edited by volunteering students from several different countries and reflects the broader internationalisation of law.

MISSION

The Groningen Journal of International Law aims to promote knowledge, innovation and development. It seeks to achieve this by serving as a catalyst for author-generated ideas about where international law should or could move in order for it to successfully address the challenges of the 21st century. To this end, each issue of the Journal is focused on a current and relevant topic of international law.

The Journal aims to become a recognised platform for legal innovation and problem-solving with the purpose of developing and promoting the rule of international law through engaging analysis, innovative ideas, academic creativity, and exploratory scholarship.

PUBLISHING PROFILE

The Groningen Journal of International Law is not a traditional journal, which means that the articles we accept are not traditional either. We invite writers to focus on what the law could be or should be, and to apply their creativity in presenting solutions, models and theories that in their view would strengthen the role and effectiveness of international law, however it may come to be defined.

To this end, the Journal requires its authors to submit articles written in an exploratory and non-descriptive style. For general queries or for information regarding submissions, visit www.grojil.org or contact groningenjil@gmail.com.

Groningen Journal of International Law ISSN: 2352-2674 KvK: 57406375

Groningen Journal of International Law

Privacy in International Law: Regulating the Internet
volume 2, issue 2

Table of Contents

The Internationalisation of Information Privacy: Towards a Common Protection

Bo Zhao*

Keywords
INTERNATIONALIZATION; INFORMATION PRIVACY; DATA PROTECTION; INTERNET; COMMON LIFE EXPERIENCE

Abstract
The conventional view of privacy, at least shared among privacy scholars, is that privacy is a rather culture—dependent issue and would be interpreted much differently in various jurisdictions. Though this is pretty true in the pre—digital age, the scenario may have been under considerable change due to the fact of the creation of new social spheres and life experience by numerous new technologies in the digital age. The popular use of the Internet, portable devices, smart phones, geographical location devices, smart home facilities, as well as the accompanied exploitation of big data collected from such devices, create a new living environment or life structure in which personal data become highly valuable in market economy and critical for personal development. Not only our perception of privacy needs update in order to follow the new reality, but also people will acquire more commonly—shared life experience, sensibility and consciousness of one perspective of privacy: information privacy. Such commonalities consequent to living in the information age against the backdrop of escalating privacy invasion, all contribute to a more commonly accepted concept of information privacy; therefore the internalization or universalization of information privacy that is attributed to a more common life structure based on information digitization and connected networks and has long run impacts on our life and laws.

This short article intends to explore this new tendency, namely the internalization (or universalization) of information privacy, in both life realities and different legal systems. It will first discuss what and how the digitalization of human life has contributed to a more shared life experience among human beings based on the increasing connectivity, and how this further enables or generates a common perception of information privacy across the world. Second, the article will explore how the recent legal developments in both domestic laws and international laws adapt to the new life realities beyond cultural difference and political divergence. For this purpose, definitions of information privacy are compared from different jurisdictions, International policy and law documents analysed, and various court verdicts discussed, showcasing the internalization tendency of information privacy. Last, the article proposes a coherent protection of information privacy in International law to remedy the present gridlock in improving Internet Governance after Snowden's revelations.

---

* As a native Chinese, Bo Zhao is a legal philosopher by training and currently a senior research fellow at the STeP Research Group (Security, Technology and e-Privacy) at the European and Economic Law Department of the Faculty of Law, University of Groningen. The author is most grateful to his colleagues M.J. van Wolferen and C. Kaiser at the European and Economic Law Department for their valuable comments on the first draft, as well as to the editors of the Journal for their excellent editorial work.

I. Introduction

The conventional view of privacy, at least shared among privacy scholars, is that privacy is rather culture-dependent and would be interpreted much differently in various jurisdictions. Though this is pretty true in the pre-digital age, the scenario has been under considerable change due to the fact of the creation of new social spheres and life experience by numerous modern technologies in the digital age. The popular use of the Internet, portable devices, smart phones, geographical location devices, smart home facilities, CCTV, as well as the accompanied exploitation of the big data collected from such devices, have created a new "living environment" or "life structure" in which personal data has become highly valuable in a market economy, and critical for personal development.

In light of this, not only our perception of privacy needs updating in order to adapt to the new reality, but also people will acquire more commonly-shared life experience, sensibility and consciousness of one particular perspective of privacy: information privacy.[1] Such commonalities consequent to our living in the information age against the backdrop of escalating privacy invasions, all contribute to a more commonly accepted concept of information privacy. The internationalisation of information privacy is therefore attributable to a more universal life structure based on information digitisation and connected networks. The internationalisation or universalisation of information privacy certainly has made long-term impacts on our lives and laws.

This short essay intends to analyse this new tendency, namely, the internationalisation (or universalisation) of information privacy worldwide, in the context of life realities and different jurisdictions. Section II will discuss three leading cases from both sides of the Atlantic, illustrating how three of the world's top courts have enhanced the protection of information privacy in three sensitive circumstances when information privacy has been under threat. These courts' verdicts explain the circumstances to which information privacy is of close concern. Section III will discuss the way in which the popular use of new technologies has contributed to more shared life experiences, and how this further enables or generates a common perception of information privacy. Section IV analyses how international society and nation States have started to adjust to new life realities beyond cultural differences and political divergence. For this purpose, international policy and law documents are analysed, domestic law developments for information privacy across the world addressed, and difficulties illustrated, with the purpose of drawing a picture of the internationalisation tendency of information privacy protection. The last section proposes a coherent protection of information privacy in international law to remedy the present gridlock in improving Internet governance after Snowden's revelations.

II. Three Leading Cases on Information Privacy

Most recently, three world top courts from both sides of the Atlantic have taken similar steps to strengthen information privacy protection. The cases of *R. v. Spencer* and *Riley v. California* protect information privacy against unauthorised searches by law enforcement forces in criminal investigations.[2] The Google Spain case protects, or over-protects,

---

[1] This short essay uses data privacy and information privacy interchangeably, although their difference shall not be ignored in other contexts.

[2] Supreme Court of Canada, *R. v. Spencer*, 2014 SCC 43; US Supreme Court, *Riley v. California* 573 U.S.,

personal information against online dissemination via search engines that is against the appellant's will. Their decisions will have long-term impacts on both domestic laws and other jurisdictions.

In Google Spain, the European Court of Justice took a critical step towards a much stricter protection of personal data of citizens of the European Union (EU).[3] Among other issues, an important underlying rationale of this decision was to establish boundaries for search engines such as Google which are capable enough to offer 'a structured overview of the information relating to that individual that can be found on the Internet', 'information which potentially concerns a vast number of aspects of his private life', and information 'to establish more or less a detailed profile of him'.[4] The Court recognised the capacity of search engines in offering structured information concerning a data subject as interference with his or her private life, and defined Google's operator as being a data controller under Article 2(d) of the EU Data Protection Directive 95/46 (DPD).[5]

The Court's decision thus directly regulates search engines as data controllers controlling, aggregating and processing personal data according to certain preferred manners and purposes.[6] A direct consequence is that this decision will prevent personal information regarding our past, from drifting on the Internet like skims on the surface of life. This is because 'without the search engine', such personal information 'could not have been interconnected or could have been only with great difficulty'.[7] A strict implementation of this decision would end up with the situation, probably preferred by the Court, that part of our past can be suppressed or hidden from our present, upon the request of data subjects, so that we may have better control over private life and more personal autonomy. The decision empowers EU residents to control personal images or reputations in order that they are not be 'ill-judged' by others as seen in the present case based on 'segregated information'.[8] Looking from this perspective, the Court helps preserve a conventional lifestyle of the pre-digital age that is characterised largely by information segregation or 'scattered facts'.[9]

The decision was made at a critical moment of EU's data protection law reform which is comprised of a series of determined efforts to enhance personal data protection in the post-Snowden era. It is also worth noting that in April 2014 the Court declared the 2006 Data Retention Directive[10] invalid,[11] which allows Internet service providers (ISPs) to

---

___ (2014).

3 European Court of Justice, C-131/12 *Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317.

4 *Id.* para. 80.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

6 *Google Spain*, *supra* nt. 3, paras. 33–41, 80. Although 'a particular order of preference' (para. 41) in search engines' data processing can be defined differently by the American court as 'editorial judgment', enjoying free speech right protection under the First Amendment of the US Constitution. See United States District Court, *Jian Zhang et al. v. Baidu.Com Inc.* 932 F.Supp.2d 561 (S.D.N.Y. 2013), paras. 6–7.

7 *Google Spain*, *supra* nt. 3, para. 80.

8 As well as irrational decision making due to digital remembering. See Mayer Schönberger, V., *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton, 2011, 113–117.

9 The phrase 'scattered facts' is borrowed from Anita Allen. See Allen A. L., "Dredging up the past: Lifelogging, Memory, and Surveillance", *The University of Chicago Law Review*, vol. 75, 2008, 47–74, 63.

10 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive

store users' information for a prescribed time. Moreover, the decision can be interpreted with two other leading cases, both addressing similar common challenges from new information and communications technologies to information privacy protection: *Riley* and *Spencer*. These cases were unanimously decided by the US Supreme Court and the Canadian Supreme Court respectively. The two leading courts give clear gestures thereby securing the information privacy when violated by law enforcement activities.

In *Riley*, the US Supreme Court judged that the inspection of the digital data contained in an arrestee's cell phone involves 'substantial privacy interests',[12] and 'the police generally may not, without a warrant, search digital information on a cell phone seized' from an arrestee.[13] It is worth noting the comparisons made by the Court between cell phones (in particular smart phones), with traditional information containers such as diaries and documents. The Court is formally engaging itself in addressing the big changes brought up by new technologies to human life and challenges to privacy protection in law enforcement with rules and procedures from the pre-digital age. To cite Justice Alito's concurring opinion, 'we should not mechanically apply the rule used in the predigitial era to the search of a cell phone'.[14]

The Court affirmed first that modern cell phones are not just telephones, but 'in fact minicomputers that also happen to have the capacity to be used as a telephone'.[15] They can be called 'cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers'.[16] Their functionalities and the immense storage capacity, including even 'the most basic phones', can 'hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on'.[17] And these have direct consequences for privacy, the Court made three observations: first, the combination of various information can reveal more of a holder's life; second, the capacity of cell phones allow one type of information to convey more about one's life than previously possible; and third, data on a phone can be dated back to the purchase of the phone, or even earlier.[18] Cell phones differ from physical records not only by quantity, but also by quality in that GPS instruments and Internet surfing activities may reveal more about private interests and concerns and daily locations, enabling reconstruction of one's life details.[19] This shall be complicated further by the popularly used apps to manage many aspects of life and the personal data stored either on a phone or via the phone in the connected clouds.[20]

In short, the Court found that '[a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.'[21] The Court pointed out the importance of cell phones in modern life and the privacy concern of most Americans based on empirical studies that those carrying no mobile phones are the

2002/58/EC.

11 European Court of Justice, Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* ECLI:EU:C:2014:238.

12 *Riley*, *supra* nt. 2, para. 3.

13 *Id.*, para. 4.

14 *Id.*, Section B.

15 *Id.*, para. 17.

16 *Ibid*.

17 *Ibid*.

18 *Ibid*.

19 *Ibid*.

20 *Id.*, paras. 19–21.

21 *Id.*, paras. 20–21.

exception and 'it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives'.[22] The popular use of mobile phones (smart phones) has changed the privacy scenario in the sense that the gravity of privacy protection has been shifting to information privacy, if compared with a conventional lifestyle.

In *Spencer*, the Canadian Supreme Court confirmed a strong protection of Canadian Internet users' information privacy, namely, their identifiable personal information held by ISPs and the related anonymity against law enforcement activities without prior judicial authorisation when investigating online child pornography downloading and sharing activities. The verdict is a strong message to Internet privacy protection. The Court declared that

> Informational privacy is often equated with secrecy or confidentiality, and also includes the related but wider notion of control over, access to and use of information. However, particularly important in the context of Internet usage is the understanding of privacy as anonymity.[23]

The Court has clarified the importance of anonymity as one of important means for online privacy in the Internet age,[24] and 'one of the defining characteristics of some types of Internet communication'.[25] It ruled that

> the issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography, but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purposes.[26]

Anonymity is a key aspect in ensuring individual privacy in public spaces in which nobody knows a person, although he or she is just among the public, with the expectation of privacy recognised under the current legal framework inherited from the 20th century.[27] However, unlike many would have assumed and despite the Court's intentions, although law enforcement agencies will need special permission to access personal information in the near future following its verdict, anonymity in general offers no guarantee of privacy security alongside fast developing digital technologies. With or without IP addresses, the anonymity myth does not itself stand, because there are a plenty of ways to identify Internet users.[28] The Internet thus provides users with no traditional public sphere protected by anonymity in a strict sense; it is but a place where a visitor is traceable eventually unless more complex technologies are involved in surfing such as Tor.[29]

---

[22] *Id.,* para. 19.

[23] *Spencer, supra* nt. 2, 4–5 (emphasis added); see also paras. 41, 45.

[24] *Id.,* paras. 34–37, 41–43.

[25] *Id.,* para. 45.

[26] *Id.*, para. 36.

[27] Basically, a place-based legal framework according to Koops. See Koops, B.-J., "On legal boundaries, technologies, and collapsing dimensions of privacy", *Politica & Società* , vol. 12, 2014, 247–264.

[28] See in general Schwartz, P. M. and Solove, D. J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *New York University Law* Review, vol. 86, 2011, 1814–1984, 1836–1839.

[29] Tor is the privacy enhancing technique that 'allows people and groups to improve their privacy and

The three information privacy invasion cases not only demonstrate the judicial recognition of and response to the big changes or challenges of new technologies to human life, but also more attest to a certain commonly-shared, underlying consciousness among the three top courts to strengthen legal protection.

III. Information Privacy as Mutual Life Experience

As the Canadian Supreme Court claimed in *Spencer*, 'Internet users do not expect their online anonymity to cease when they access the Internet outside their homes, via smart phones, or portable devices.'[30] According to the European Commission, the Internet has become a 'general purpose technology and a basic and essential element of any all citizens' life'.[31] The Finnish State has listed access to the Internet as a legal right,[32] like the critical public services of electricity and drinking water supply provided by government. The Council of Europe expressed explicitly in a recent resolution that '[a]t present, the prevailing opinion is that access to Internet should be recognised as a fundamental right.'[33] The use of the Internet has been an important part of human life on daily basis in the information age and users have legitimate expectation of privacy while engaging in online activities. Globally speaking, information privacy becomes increasingly important given that about 40% of the world population has access to the Internet nowadays.[34]

The crucial role of mobile phones (especially smart phones) in American's daily life as pointed out in *Riley*, is no exception to the rest of the world. For example, in both the EU and China, two large economies, smart phones have become increasingly important as a means to seek information and instant communications, manage personal data, and self-entertain.[35] Up to 2017, mobile phone users will increase from 61.1% to 69.4% of the

---

security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.' See: Tor, *About Tor*, available online at <torproject.org/about/overview.html.en> (accessed 30 November 2014).

30 *Spencer, supra* nt. 2, para. 37.

31 See Action 97, *Promote the internationalization of internet governance*, available online at <ec.europa.eu/digital-agenda/en/international/action-97-promote-internationalisation-internet-governance> (accessed 11 October 2014).

32 From 2010 with a legal right to a 1 Megabit per second (Mbps) access connection; and in 2015, everybody shall have 100 Mbps connections, according to a commitment of the legislator. See Ermert, M., "Internet: Finland running ahead on access and democracy", *Internet Policy Review*, available online at <policyreview.info/articles/news/internet-finland-running-ahead-access-and-democracy/218> (accessed 11 October 2014).

33 Council of Europe, Committee on Culture, Science, Education and Media, Pelkonen, J., REPORT: *The right to Internet access*, Doc. 13434, 4 March 2014, 7.

34 See Internet live stats website, available online at <internetlivestats.com/internet-users/> (accessed 11 October 2014).

35 In China, there are about five billion cell phone users and 81% of 6.18 billion Internet users were going online via mobile phones in 2013. See China Internet Network Information Centre, REPORT: *Report on China's Internet Development in 2013*, January 2014, 5, available online at <www1.cnnic.cn/IDR/ReportDownloads/201404/U020140417607531610855.pdf> (accessed 11 October 2014). Regarding Europe, 49% of the 4.03 billion European mobile phone users had smart phones in 2012. See GSMA, *The Mobile Economy Europe 2013*, 11, 17, available online at <gsmamobileeconomyeurope.com/GSMA_Mobile%20Economy%20Europe_v9_WEB.pdf> (accessed 11 October 2014)

world population.[36] Because of multi-functionality and portability, smart phones are reconstructing or will be reconstructing our lifestyle, in particular with respect to young generations. They increasingly function as the focal point of personal data, due to the big data storage capacity and connectivity capacity allowing personal information to be accessed and stored elsewhere. Other portable devices like laptops and tablets play no less a role in getting people connected, aggregating equally personal data via various apps for different purposes, with or without users' consent.

Google Spain reflects another aspect of the new technologies in revolutionising our information/knowledge structure. This is because the algorithms used by search engines decide on what would be read by most Internet users who have no capacity to trawl through the connected networks themselves. As intermediaries, the rising power of search engines represented by Google is decisive in what kinds of personal information are available for searchers, so that you are what Google says you are,[37] and our reputation and privacy are in their hands. Furthermore, search engines gain accumulative power in profiling and computing the data left by users, either to improve services such as targeted advertisements and search results and to predict big public health events,[38] or other services unknown to users. The point is that on many occasions our online surfing does mean starting with "Googling".

The popular use of the Internet, new telecommunications devices and new technologies in data processing, as partially revealed above, are playing more and more important roles in daily life. Technologies used in new telecommunication and computer devices, innovative software, new apps, social networking services, monitoring devices (cheap sensors), fibre optics, Wi-Fi, etc. are constructing our new life or reconstructing our old life on a large scale, by creating a new living environment. Our life structure has been changed with similar patterns, and we will consequently gain more mutual understandings of information privacy. The core of information privacy, as the Court noted in *Spencer*, is 'a wider notion of control over, access to and use of information'.[39]

Above all, our daily life has somehow shifted gradually into the online sphere where we spend considerable time engaging in all kinds of Internet-related activities. This does not mean that our offline, physical life is no longer important. Instead, it means that the traditional analogue world becomes a more basic thing, in the way that it is increasingly restructured and reorganised by means of connected networks. Connected networks provide important means such as real time information (data) and organisational platforms to support various social activities, ranging from booming e-business, flash mobs, to cross-continent family Skype gathering, to political movements, even military actions, etc.

Another prevailing trend is the forthcoming "big data age" in which data processing becomes the premise of decision making at different levels. This is true at the national level where national policies have to be made based on more empirical data; at the

---

[36] See Emarket, REPORT: *Smartphone Users Worldwide Will Total 1.75 Billion in 2014*, January 2014, available online at <emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536> (accessed 11 October 2014).

[37] Ambrose, M., "You are What Google Says You are: The Right to Be Forgotten and Information Stewardship", *International Review of Information Ethics*, vol. 17, 2012, 21–30.

[38] Google successfully predicted the regional spread of winter flue in the US and the 2009 N1H1. See Mayer-Schönverger, V. and Cuiker, K., *Big Data: A Revolution That Will Transform How We Live, Work and Think*, John Murray, London, 2013, 1–3.

[39] *Spencer, supra* nt. 2, para. 40.

business level where more companies adjust business strategies according to collected consumer data; and at personal level where more personal decisions are made on accessible data collected by smart watches, smart metering devices, Google maps, live weather forecast, shopping apps, business reputation webs, etc. Data-based decision-making requires more detailed data and the precision necessary for making rational decisions.

Therefore, a gradually recognised life reality is the increasing value of personal data/information in the digital age, or the proprietary nature of the information economy.[40] Google and other tech vendors have efficient ways to exploit the big data collected from the data-for-service business model. As Viviane Reding commented, '[p]ersonal data is the currency of today's digital market.'[41] The commercial value in personal data has led to large scale global trade in personal,[42] which draws attention to information privacy invasion and the illegal trade in private information. The problem now is that while users surf the Internet, they may not even notice data collection conducted by a number of techniques including popular cookies and most recently canvas fingerprinting.[43] With added value in personal information, the ownership of personal information/data has become a haunting problem to be decided later, and the identification of ownership would be a crucial issue in the information decade.

Furthermore, what comes with this new life structure is an increasingly mutual consciousness of being connected and information sharing (connectivity and sharing).[44] One can choose to interact with the strangers of life, in particular celebrities one adores, via social networking services or with institutions by subscribing to their group mail services or Facebook or Twitter accounts. The sense of being connected and connecting to the rest of the world, non-exclusive to humans,[45] assists us with reorganising our communications and life structure, opening the door for sharing. Sharing, whether via Facebook, Google +, Twitter, or Instagram, Skype, or other social networking tools, has been creating more common life experiences across the world.

An illustrative analogy would be the invention and spread of paper books which led to the commonly shared experience of reading, though people might read books with different contents and in different languages. The common sense of "reading a book" is very much the same everywhere when we refer to the activity of reading. A recent story

---

[40] As such, in the discussion of personal information from proprietary perspective see for example: Lessig, L., "Privacy as Property", Social Research: An International Quarterly, vol. 69, 2002, 247–269; Murphy, R. S., "Property Rights in Personal Information: An Economic Defense of Privacy", *Georgetown Law Journal*, vol. 84, 1995, 2381–2418.

[41] European Commission, Vice-President of the European Commission, EU Justice Commissioner, Viviane Reding, PRESS RELEASE: *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, 22 January 2012, SPEECH/12/26, available online at <europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26> (accessed 12 November 2014).

[42] For example see the story revealed in the interview of CBS of big data brokers in the United States famous for strong personal information profiling. CBS, Kroft, K., *The Data Brokers: Selling Your Personal Information*, 9 March 2014, available online at <cbsnews.com/news/the-data-brokers-selling-your-personal-information> (accessed 13 November 2014).

[43] PC World, Kirk, J., *Researchers Reveal 3 Devious Ways Online Trackers Shatter Your Digital Footsteps*, 22 July 2014, available online at <pcworld.com/article/2456640/stealthy-web-tracking-tools-pose-increasing-privacy-risks-to-users.html> (accessed 13 November 2014).

[44] Just recall how often many of us check emails and mobile phones a day to have the feeling of "being connected" or "sharing" or "being kept up-to-date", even shortly before going to sleep or at any moment if connected.

[45] In the sense of man-to-machine and machine-to-machine, or a combination of both.

exemplifying the strong need for "sharing" and "being connected" is a Russian soldier's sharing of his Instagram pictures taken within a BUK with the whole world,[46] which inflamed the already contentious MH17 disaster at a particularly politically sensitive moment.[47] The construction or re-construction of human life will accelerate when the Internet of Things (IoT) becomes a reality in the near future, in that everything will be inter-connected.[48]

Last, the widespread and provoking data protection invasions have greatly contributed to a common recognition of the significance of information privacy across the world. Snowden's major revelations demonstrate how a State, using modern technologies, is capable of conducting mass surveillance of its citizens and beyond its borders in the name of public security. New technologies make mass surveillance possible in the digital age at a scale unimaginable before, enabling State authorities to be giant data controllers and the number one threat to information privacy. However, more tangible threats to Internet users are from cybercrimes including online fraud, online stalking, and identity theft. They are easier to perform and relatively harder to trace by law enforcement agencies than traditional crimes. The increasing awareness of the need to protect personal privacy can be easily observed in empirical studies of Facebook users who tend to disclose less personal information today compared to the past.[49]

What has accompanied the awareness of information privacy among new technology users is sensitivity to the gradual collapse of two traditional separations in daily life: the separation between the past and the present, and the separation between the public and the private. The breakdown of the first impedes personality and identity development, given that one's past continues to pervasively influence the present. This problem has been partially addressed by the "right to be forgotten" proposed in the new EU General Data Protection Regulation,[50] and partially by the Google Spain. The second breakdown concerns situations of, for example, the blending of home and work among those tele-workers for whom privacy is of a big concern nowadays. The collapse of the separation between the public and the private causes the dilution and evaporation of the boundaries of private life, giving birth to what Koops described as 'the collapse of the privacy boundaries'. [51] The firm separation between time and space somehow seems malleable or breakable in many contexts.

---

[46] The anti-aircraft missile system developed by the Soviet Union.

[47] The Guardian, Jones, J., *A Russian soldier's "Ukraine selfies" are not evidence, they're war art*, 1 August 2014, available online at <theguardian.com/commentisfree/2014/aug/01/russian-soldier-alexander-sotkin-instagram-ukraine-selfies> (accessed 16 August 2014).

[48] Due to the pervasive computing ability based on the merge of the physical world and analogue world. See in general: The Guardian, Singh, J. and Powles, J., *The internet of things - the next big challenge to our privacy*, 28 July 2014, available online at <theguardian.com/technology/2014/jul/28/internet-of-things-privacy> (accessed 11 August 2014).

[49] An empirical study of the Facebook users in the US from 2005 to 2011 shows the decreasing amount of personal information shared publically with unconnected profiles, although the default policy of Facebook eventually produces more disclosure over time. See: Stutzman, F., *et al*., "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook", *Journal of Privacy and Confidentiality*, vol. 4, ed. 2, 2012, 7–41available online at <repository.cmu.edu/jpc/vol4/iss2/2> (accessed 13 November 2014).

[50] For a detailed analysis of the right, see: Shoor, E., "Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation", *Brooklyn Journal of International Law*, vol. 39, 2013, 491–494, available online at <papers.ssrn.com/abstract=2410240> (accessed 16 August 2014).

[51] See Koops, *supra* nt. 27, Part 3, Surveillance and the Boundary of Private Space, for an analysis of the merging of private and public places consequent to new surveillance technologies.

All in all, Internet and telecommunications technologies have gradually developed a new life structure accompanied by experiences in human life that did not exist before. The consequences include the homogenous consciousness and sensitivity of "being connected or connecting" and "sharing" with others, together with the increasing acknowledgement of the importance of information privacy in personal life. The commonalities could be explained by previous similar technical revolutions such as in publishing, TV and the auto industry, in the sense that the life experiences and understandings of "driving a car" and "watching TV" and "reading a book" would not be much different, whether one was Chinese, African, or European.

With respect to the digital age, this can be attributed to the "inter-connectivity" of connected networks and the "digitalisation of personal information" (among other related information). Digitalisation of personal data enables personal information to be easily transported and archived by individuals, while connectivity or inter-connectivity allows collected data to be easily gathered, aggregated, distributed and processed, even when scattered at different geographical locations. Both help with breaking down the time and spatial limits within human physical life.

IV. The Internationalisation of Information Privacy

The new life structure and the incurred common life experiences and sensibility lead to increasingly mutualised understandings of privacy, in particular information privacy. The importance of information privacy as a fundamental right has not only been recognised by the three leading courts, but also well addressed by the international community and many national laws.

At the UN level, the General Assembly adopted Resolution 68/167 in December 2013, affirming that 'the same rights held by people offline must also be protected online 'calling upon' all States to respect and protect the right to privacy in digital communication'.[52] As 'the first internationally agreed upon statement of core information privacy principles',[53] the previous OECD privacy guidelines had a major influence on member States' privacy protection laws,[54] and was substantially consistent with Convention 108 of the Council of Europe;[55] though its influence on the EU DPD is unclear, both enjoy 'many of the same basic principles'.[56] The OECD privacy guidelines were updated and revised last December in light of 'changing technologies, markets and user behaviour, and the growing importance of digital identities'.[57]

The OECD privacy guidelines are instrumental to the development of the privacy protection framework of the Asia-Pacific Economic Cooperation forum (APEC), which bears many similar information privacy principles with the former.[58] Similarly, the DPD

---

[52] GA Resolution 68/167 (68th session), A/RES/68/167, 21 January 2014, adopted by the General Assembly on the Report of the Third Committee, The Right to Privacy in the Digital Age, GA Resolution A/68/456/ADD.2, 18 December 2013, available online at <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167> (accessed 13 November 2014).

[53] OECD, *The 2013 OECD Privacy Guidelines*, no. 76, available online at <oecd.org/sti/ieconomy/privacy.htm#newguidelines> (accessed 13 November 2014).

[54] *Id.*, 77–78.

[55] Council of Europe (CoE), Convention for the protection of individuals with regard to automatic processing of personal data, 1981 CETS No. 108.

[56] The 2013 OECD Privacy Guidelines, supra nt. 53, 80.

[57] *Id.*, 3.

[58] *Id.* 80. Also see Greenleaf's discussion of their relationship: Greenleaf, G., "The Influence of European

has influenced other jurisdictions according to a study conducted by Greenleaf.[59] The internationalisation of information privacy protection shall ultimately include member States of the Economic Community of West African States (ECOWAS) which adopted a Supplementary Act on Personal Data Protection within ECOWAS in 2010 with clear influences from the EU DPD. Furthermore, Convention 108 should be mentioned because of its significance. The Convention has been strengthened by the 2001 Additional Protocol (ETS 181) which includes data export restrictions and a remedy mechanism.[60] With forty-three member States having ratified the convention and forty-two having signed the Additional Protocol (with thirty-one ratifications), Convention 108 has been open to accession since mid-2008.[61]

The three leading cases discussed above showcase the common tendency towards strengthening information privacy protection, although they have very different cultural conceptions of privacy.[62] Ms. Falque-Pierrotin, Chair of the Working Party on Article 29, in replying to an advisory report for President Obama, said that 'a number of guidelines it has issued in recent months … are also consistent with the analysis of some privacy concerns which are identified in the report'; which includes its opinions on anonymisation techniques, application of necessity and proportionality principles, data protection within the law enforcement sector, legitimate interest, purpose limitation, open data and public sector information re-use, etc.[63]

Having realised the importance of personal data protection for the information economy and individual life, many jurisdictions have passed legislation protecting personal data in the last decade. According Greenleaf, up until 2012 there were 81 countries providing comprehensive data privacy protection coverage over both the public sector and private sector, with a set of basic privacy principles approximating the OECD privacy guidelines or the Council of Europe 108 Convention, together with some methods of statutorily-mandated enforcement.[64] In 2012 the author still could not predict in which direction China's privacy law would head.[65] But at this moment it seems clear that the Chinese State authority has made great efforts to enhance data privacy protection upon realising the importance of the information economy to China's future prosperity and further economic growth.[66] Recently, the EU has taken a significant step towards strengthening data protection with the proposed new data protection package.[67]

Data Privacy Standards Outside Europe: Implications for Globalisation of Convention", *International Data Privacy Law*, vol. 2, ed. 2, 2012, 68–91.

59 *Id.*, 73–81.

60 *Id.,* 86–87 discussing the Council of Europe (CoE) Convention 108, the Convention for the protection of individuals with regard to automatic processing of personal data.

61 *Id.,* 88. Uruguay is the first non-CoE State accessed. See: FRA, *Handbook on European Data*, 16, Publications Office of the European Union, 2014, available online at <fra.europa.eu/en/publication/2014/handbook-european-data-protection-law> (accessed 25 August 2014).

62 See in general, Whitman, J. Q., "Two Western Cultures of Privacy: Dignity versus Liberty"*, Yale Law Journal*, vol. 113, ed. 6, 2004, 1151–1221.

63 Out-Law, *EU Privacy Watchdog to Conduct Review of Big Data Potential Within Existing Legal Boundaries*, 14 July 2014, available online at <out-law.com/en/articles/2014/july/eu-privacy-watchdog-to-conduct-review-of-big-data-potential-within-existing-legal-boundaries/> (accessed 13 November 2014).

64 Greenleaf, *supra* nt. 58, 69.

65 *Id.*, 73.

66 In particular by means of a series of public policies and the amendment of China's consumer law responding to the massive abuse of personal data in China's booming e-business. For a brief review, see: Privacy and Information Security Law Blog, Hunton & Williams LLP, *China Passes Amendment to Consumer Protection Law*, 28 October 2013, available online at

The legal protection provided by domestic laws is much easier to initiate, promulgate and implement due to the more common interests and political background within a single State. At the UN level, agreement or consensus regarding general principles of data protection are not difficult to reach when this concerns only political statements and declarations without the necessity of further substantial measures being taken.

However, the situation is quite different in cases where major substantial interests come into play and international cooperation is a must for data privacy protection. At this point, a telling example is trans-border data processing (i.e. clouding computing and cross-border e-commerce) which will take the issue beyond national borders and requires transnational cooperation and political efforts. This is a difficult issue when differing legal systems are combined with conflicting commercial interests and fierce business competition in bilateral or multilateral negotiations. One can imagine how much the US would be willing to compromise when, first, their laws have lower protection of personal data privacy, and, second, most of the IT and digital giants are American companies. Besides, the issues will be more complicated when political considerations are added, such as anti-terrorist surveillance measures and State espionage, demonstrated by the Snowden leaks and the most recent German's interception of the communications of Hillary Clinton and John Kerry.[68]

A much easier agreement to be reached would be in law enforcement cooperation, as both sides have similar concerns. Since 2011, the EU has participated in the Data Protection Umbrella Agreement with the US and there have already been 20 negotiations up to June 2014 covering all personal data transferred from the EU to the US in the context of the prevention, detection, investigation and prosecution of criminal offences.[69] Meanwhile, the European Commission has been engaging in the negotiation with the US to 'make the Safe Harbour scheme safer' and has made 13 recommendations to the US authorities, majority of which see substantial progress with only an exception on national security.[70]

V. Towards a Common Protection

Restoring mutual trust among State stakeholders is a precondition for any international treaty on stronger personal data protection. When mutual interests are strong enough and political considerations are not imminent, it is not difficult, at a given moment, to reach agreement between States on information privacy protection. This is seen in the first international treaty on cybercrimes promulgated by the Council of Europe and recognised by some non-European countries including the US.[71] Notwithstanding that

<huntonprivacyblog.com/2013/10/articles/china-passes-amendment-to-consumer-protection-law/> (accessed 13 November 2014).

67 Europa Nu, *Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote*, 12 March 2013, available online at <europa-nu.nl/id/vji0icq99kyp/nieuws/progress_on_eu_data_protection_reform?ctx=vhkejco8liwc&s0e=vhdubxdwqrzw> (accessed 13 November 2014).

68 The World Post, Jordans, F., *German Intel Spied on Hillary Clinton, John Kerry, Der Spiegel*, Huffington Post, 16 August 2014, available online at <huffingtonpost.com/2014/08/16/german-spying-clinton-kerry_n_5684202.html> (accessed 13 November 2014).

69 European Commission, *Factsheet EU-US Negotiations on Data Protection*, June 2014, available online at: <ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf> (accessed 14 November 2014).

70 *Ibid*.

71 Mario, N., "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation",

the treaty might be symbolic to some,[72] it is the only international treaty against cybercrime that really brings States on the same page in handling Internet-related issues. A similar approach is expected, by some scholars or even the Council of Europe, to be effective for enhancing privacy protection in particular, and Internet governance in general.[73]

Information privacy has received further protection in the world's major jurisdictions. However, information privacy protection is far from sufficient when compared with the most recent developments of Internet and communications technologies and the lack of legal remedies beyond State laws. But with more common experiences gained in our digitalised and connected modern life, international society has developed a greater consensuses and awareness of the significance of information privacy across the world. The critical moment is not far off, with more globally recognised grounds for information privacy protection and more commonly accepted standards, to define and remedy privacy violations under international law. Regarding this, it is best to conclude the article by quoting a recent speech by Holder, the US Attorney General

> The Obama administration is committed to seeking legislation that would ensure that … EU citizens would have the same right to seek judicial redress for intentional or willful disclosures of protected information and for refusal to grant access or to rectify any errors in that information, as would a US citizen under the Privacy Act.[74]

*

International Journal of Cyber Law Criminology, vol. 4, 2010, 699–712, 702.

[72] *Ibid*.

[73] See Cannataci's discussion of a possible treaty in the context of the Council of Europe. Mapping, Blogs, Cannataci, J., *Parallel Internets, Another Internet Treaty or Both? The Next Pieces of the Internet Governance Jigsaw Puzzle*, available online at <mappingtheinternet.eu/node/41> (accessed 13 November 2014).

[74] The Guardian, MacAskill, E., *et al.*, *US to extend privacy protection rights to EU citizens*, 25 June 2014, available online at <theguardian.com/world/2014/jun/25/us-privacy-protection-rights-europe> (accessed 22 July 2014).

Bridging the gap between individual privacy and public security

Rolf H. Weber[*] and Dominic N. Staiger[**]

Keywords
PRIVACY; SECURITY; ANONYMITY; HUMAN RIGHTS; RIGHT TO BE FORGOTTEN; SURVEILLANCE; DATA COLLECTION

Abstract
This article outlines the concept and origin of privacy law as it is applied today in various jurisdictions around the world. It then provides examples of governmental intervention affecting the privacy rights of individuals and critically examines their suitability and proportionality in light of the environment in which they operate. Balancing the interest of an individual's privacy against the often legitimate concerns of a government for public order requires legislators to implement laws which provide an appropriate balance between these two competing interests. Throughout the article varying approaches in setting boundaries for privacy laws are analysed and improvements suggested. Furthermore the privacy challenges created in the online world are addressed and current developments highlighted.

I. Origin and types of privacy laws

I.1. Historical origins

(i) Privacy as a notion has been part of the law since the British parliament passed the Justices of the Peace Act in 1361. It marked the beginning of the recognition of individual rights by providing for the arrest of eavesdroppers. This concept was further expanded to include a course of action for trespass in cases in which private property was seized without a warrant[1] and later a privacy interest in printed etchings, precluding reproduction without the consent of the original owner.[2]

At this point in history the arguments in favor of a privacy right were based on the concept of property, forming an integral part of any society. However, no tort for a breach of privacy has yet been recognised in the UK.[3] In contrast, over the last thirty five years the USA moved away from the concept of property as the basis for the attachment of a privacy right to a more holistic and individual focused view.[4] In Europe the

---

[*] Rolf H. Weber is Chair Professor for International Business Law at the University of Zurich, Switzerland, Visiting Professor at the University of Hong Kong, Hong Kong, and Attorney-at-Law in Zurich.

[**] MLaw Dominic N. Staiger is Assistant and PhD Student at the Chair for International Business Law at the University of Zurich and Attorney-at-Law in New York (USA).

1 *Entick v. Carrington*, 19 State Trials 1029 (1765).

2 *Prince Albert v. Strange*, 1 Mac. & G. 25 (1849).

3 Although the US and New Zealand recognise such a right. See Prosser, W. L., "Privacy", *California Law Review*, vol. 48, 1960, 338 for an analysis. Recent cases in New Zealand are *Hosking v. Runting* [2005] 1 NZLR 1 and in Canada, *Jones v. Tsige* [2011] ONSC 1475.

4 *Rakas v. Illinois*, 439 U.S. 128 (1978).

development of privacy laws has been significantly influenced by the human rights approach of the European Convention on Human Rights.[5]

(ii) William Pitt, a member of the UK Parliament vividly expressed his views on privacy in 1763

> The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter, the rain may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement.[6]

Although the law has come a long way since the 17th century,[7] the fundamental notion of privacy has remained the same. At its core lies the protection of the individual in his private sphere from interference by the state and other private actors.

(iii) The concept of privacy consists of the three main features secrecy, anonymity and solitude.[8] In particular the value attached to information varies with respect to the individual to which the information relates who generally has a higher interest in its secrecy than a potential bystander. However, privacy is valuable not only to the individual but also to a functioning democratic political system and all individuals therein as it provides a seclusion in which democracy can grow.[9]

Various factors also point to the recognition of privacy as a fundamental human need that ought to be recognised by the international community and individual countries. As a starting point the right to privacy can be found in international treaties such as the Universal Declaration of Human Rights in Article 12, which expressly protects an individual's privacy. Such a provision is also included in Article 17 of the International Covenant on Civil and Political Rights as well as Article 16 of the Convention on the Rights of the Child.

I.2. Constitutional privacy protection

With the adoption of the US Constitution the concept of privacy was further expanded from what existed at the time under British law by including a constitutional right to protection from unreasonable search and seizure by the government (4th Amendment). In particular, newer case law has found a right to privacy in marital relations through the combined force of the First, Third, Fourth and Ninth Amendment of the US Constitution.[10] In the famous Griswold case Justice Douglas formed the opinion that various constitutional guarantees create zones of privacy and are necessary in order to give the guarantees life and substance. As Justice Brandeis later put it in 1928

---

5 For current developments and judgments see European Court of Human Rights, available online at <echr.coe.int/Pages/home.aspx?p=home> accessed 10 September 2014.

6 Speech on the Excise Bill, House of Commons (March 1763).

7 The Swedish Freedom of the Press Act of 1766 was the first legislation to grant access to public documents.

8 Weber, R. H., "How does Privacy change in the Age of the Internet?", *in*: Fuchs, C., Boersma, K., Albrechtslund, A. and Sandoval, M., eds., *Internet and Surveillance*, Routledge, 2011, 274.

9 Regan, P. M., *Legislating privacy: Technology, Social Values and Public Policy*, University of North Carolina Press, Chapel Hill and London, 2009, 225.

10 *Griswold v. Connecticut*, 381 U.S. 479 (1965).

> The makers of the constitution sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men.[11]

Thus, the law on privacy has significantly progressed since its first public appearance in the famous 1890 Harvard Law Review article of Louis D. Brandeis and his fellow Harvard alumni Samuel D. Warren.[12] Both argued for the first time in an academic publication that a broader concept of privacy existed to protect individuals against outrageous and unjustifiable infliction of mental distress. Although, at first sight, later cases did not follow this view out of fear of the vast amount of litigation and the difficulty in drawing a line between public and private figures, it forms a cornerstone to privacy law development in the US.[13] Today, privacy rights in regard to slander and libel are recognised in American state statues[14] as well as in case law. Ten state constitutions expressly recognize a right to privacy whereas this right has also been found in states without constitutional privacy protection by way of court judgments.[15]

The UK does not have a constitution, therefore the passing of the US Constitution was the first time in common law history a citizen could point to a constitutional limitation on a state's power in regard to an individual's personal rights. The growing privacy protection in UK law was mainly influenced by the legislative action on the European level such as the European Convention on Human Rights and Fundamental Freedoms (ECHR) as well as the European Union (EU) treaties.

In contrast to the European and US approach, in Latin America[16] a separate constitutional remedy named Habeas Data has been introduced. It allows an aggrieved data subject to seek a court remedy in form of injunctive relief or damages and requires a request to access the data stored in the target database. Today, many constitutions such as the amended constitution of Brazil include an inviolable right to privacy.[17] By clearly stating such a right in the highest legal instrument a signal is sent to the government agencies to carry out their tasks in accordance with privacy laws and allows aggrieved citizens to point to a directly enforceable right. In how far these rights are effective in the South American countries remains to be seen.

---

[11] *Olsmtead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., Dissenting Opinion), the majority found that wiretapping did not involve "tangible" things and thus did not afford the constitutional protection. This case has later been overruled. See also Warren, S. and Brandeis, L., "The right to Privacy", *Harvard Law Review*, vol. 4, ed. 5, 1890.

[12] Warren, S. and Brandeis, L., "The right to Privacy", *Harvard Law Review*, vol. 4, 1890.

[13] *Roberson v. Rochester Folding Box Co*. 171 NY 538, 64 NE 442 (1902).

[14] Article 5, Section 50, New York Civil Rights Law.

[15] National Conference of State Legislatures, *Privacy Protections in State Constitutions*, available online at <ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx> (accessed 10 September 2014).

[16] Including the countries Brazil, Mexico, Peru, Argentina and Paraguay.

[17] Article 5, Section 10, Constitution of the Federative Republic of Brazil, available online at <stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/constituicao_ingles_3ed2010.pdf> (accessed 10 September 2014).

I.3. European and international human rights approach to privacy

In Europe the concept of privacy is officially part of the broader legal system based on the European Convention on Human Rights and Fundamental Freedoms (Article 8).[18] It provides for a right to respect of one's private and family life, one's home and correspondence. The European Court of Human Rights (ECtHR) has further defined the concept of privacy through its judgments. For example, the French case of *A v. France* highlighted that a telephone conversation does not lose its private character solely because its content concerns public interest.[19] Emphasis was placed on the requirement that the investigating judge must issue a specific order[20] for the measure and the approved order must be 'necessary in a democratic society'.[21]

Furthermore, the fundamental rights to privacy and security are included in Article 6 and 7 of the Charter of the Fundamental Rights of the European Union.[22]

Once a breach of the right to privacy has been established, the determination of the applicable remedy becomes a central issue, especially in a search and seizure situation as the evidence obtained can result in the acquittal or conviction of a person. In Europe the Convention requires an 'effective remedy' to be implemented into the national law of every signatory to the Convention.[23] What constitutes an appropriate remedy is, however, left to the national state legislators and courts to decide.

On the American continent the American Convention of Human Rights also includes in Article 11 a right to privacy.[24] Importantly, none of the treaties or agreements recognises privacy to be an absolute right.

The term "arbitrary interference" is used in many of the international treaties and conventions and forms part of a balancing exercise between legitimate interference on justifiable grounds and arbitrary interference. In this regard the Inter-American Commission of Human Rights has offered an interpretation by referring to 'elements of injustice, unpredictability and unreasonableness, and proportionality of the searches and inspections'.[25] The practical use of this expression remains questionable due to its vagueness.

In addition to formal treaties or agreements, rights can also be recognised under customary international law. For example, international conventions can be a source of customary international law as they represent the agreed upon base line for a specific issue throughout the majority of countries in the world.[26]

---

[18] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 (ECHR).

[19] ECtHR, 23 November 1993, *A v. France*, 14838/89, 52.

[20] ECtHR, 10 July 1998, *Valenzuela Contreras v. Spain*, 27671/95, 70.

[21] Article 8 ECHR.

[22] Charter of the Fundamental Rights of the European Union, 2000, 2000/C 364/01,

[23] Article 13 EHCR.

[24] Organization of American States (OAS), *American Convention on Human Rights, 'Pact of San Jose',* Costa Rica, 22 November 1969.

[25] Inter-American Commission on Human Rights, REPORT: *81st Session Annual Report 1996*, 14 March 1997, Case 10.506, Rep. No. 38/96, Washington DC, 92.

[26] Shaw, M. N., *International Law*, 5th ed., Cambridge University Press, Cambridge, 2003, 54–82.

I.4. Boundaries of privacy and security

Under international law, the state is burdened with the duty to serve as the guarantor of human rights. States can therefore restrict individual rights such as the right to privacy on the grounds of general welfare, the protection of other fundamental rights, public morality or security.[27] In doing so they must balance an individual's right to privacy against the general welfare of society.[28]

The International Court of Justice has highlighted that the government acts concerned must not 'only amount to settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it.'[29] Furthermore, governments need to take into account that any action taken by them affecting privacy that leads to a change in behaviour of citizens can be considered a privacy violation when privacy is defined as the 'freedom from unreasonable constraints on the construction of one's identity'.[30]

Since a balance between privacy and security advocated in this paper can only be achieved when a society and government know what degree of control is exerted, by whom and for how long,[31] the concept of security also requires clarification. At its core it encompasses the central role of every government regarding the protection of its citizens, organizations, and institutions against threats to their well-being and to the prosperity of their communities. Both the concept of security and privacy include an element of protection.[32] However, privacy focuses on the individual whereas security in its present context places its focus on protecting the public at large. Therefore, a fine line exists between protecting legitimate state interests and utilising governmental power to advance public influence through oversight and surveillance. Also the definition on public order and morals, which the state wants to maintain, varies depending on the given circumstances. Thus the views on the necessary measures and justifications differ substantially from country to country. Article 19 para. 3 ICCPR (UN 1966) clearly states that the individual rights can be infringed by laws which are necessary for the protection of public order and national security. To what extent a government can go in enforcing such a right depends in most parts on the interpretation of constitutional limitations and international human rights treaties. In light of this definition governmental security actions in relation to personal privacy infringements are highlighted hereinafter.

---

27 Article 29(2) Universal Declaration of Human Rights.

28 Rengel, A., *Privacy in the 21st Century*, Hotei Publishing, Leiden, 2014, 88.

29 International Court of Justice, 20 February 1969, *North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands)* ICJ Reports 1969, 3, para 77.

30 Agre, P. E., and Rotenberg, M., *Technology and Privacy: The New Landscape*, MIT Press, Cambridge, Massachusetts, 2001, 7.

31 Westin, A., *Privacy and Freedom*, Bodley Head, London, 1970, 7.

32 Weber, R. H. and Heinrich, U. I., *Anonymization*, Springer, London, 2012, 35.

II. Privacy laws and their application to government action

II.1. Tensions between security and privacy

In today's society trade-offs between privacy and security are increasingly challenging. Fundamental rights not only aim at limiting a state's power, allowing individuals to oppose such power, but also provide its main justification in the guarantee of exactly those rights.[33] The values privacy protects are the right to dignity and freedom, the core elements of every democratic society.

It has been suggested that the right to privacy could serve as guidance when faced with an intrusive technology to define whether it should be allowed and what restrictions should be placed on it. In doing so data protection can only act as a tool to regulate the acceptable use in order to minimize the impact on fundamental rights.[34]

One of these fundamental rights questions was raised in *Norris v. Ireland* when the court had to consider whether the Irish anti-sodomy law fulfilled the requirement of being "necessary in a democratic society". This would have required a showing that the interference caused by the law "answered a pressing social need" and was proportionate to the legitimate aim pursued by the law.[35] In its judgment the court rejected the argument that the scope of the government's right to determine whether a law is "necessary" should be broadened. This strict approach to "necessity" was affirmed *in Lustig-Prean and Beckett v. United Kingdom* and has been the prevailing standard since.[36] Government action within the EU infringing on the right of privacy must therefore be closely scrutinized in light of these decisions.

The growing information technology sector and data industry have created a need to rethink and redefine the way personal data and data in general should be treated. Of particular importance is the usage of personal data which directly affects an individual in his right to privacy. A first guidance has been given in this regard through the Human Rights Committee by extending the applicability of Article 17 of the International Covenant on Civil and Political Rights (ICCPR) to personal data.[37]

Also the EU has taken a firm stance on data protection by focusing its efforts on four central pillars. These are the right to be forgotten, transparency, privacy by default and data protection regardless of location.[38] Additionally, the EU has passed the Regulation on the protection of individuals with regard to the processing of personal data by European Community (EC) institutions and bodies and on the free movement of such data. This Regulation sets boundaries on the community institutions' personal data processing capabilities when processing is carried out under community law.[39]

---

33 Chevallier, J., *L'État de droit*, Clefs Politiques, 2nd ed., Montchrestien, Paris, 1994.

34 Coudert, F., "When video cameras watch and screen: Privacy implications of pattern recognition technologies", *Computer Law & Security Review*, vol. 26, 2010, 381.

35 ECtHR, 26 October 1988, *Norris v. Ireland*, 142 ECHR 186, 198.

36 ECtHR, 27 December 1999, *Lustig-Prean and Beckett v. United Kingdom*, 29 ECHR 548.

37 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, 171 .

38 Europa Press Release Database, Speech by Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, *Your data, your rights: Safeguarding your privacy in a connected world*, 16 March 2011, Brussels, available online at <europa.eu/rapid/press-release_SPEECH-11-183_en.htm> (accessed 10 September 2014).

39 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, available online at <eur-

Of central importance to any privacy discussion is the understanding that the growing convenience provided by private and public actors in the online market comes at the price of giving away personal information and a loss of privacy. This occurs regularly with the use of Apps on mobile phones that communicate the location of the phone to the App provider, which subsequently can use this information for commercial purposes and also could be required to hand the data over to public authorities upon request.

Generally surveillance is targeted at a specific person of interest. Technological progress today allows for mass surveillance of a huge amount of individuals of which most are law-abiding citizens. This increases the tensions between balancing any legitimate state interest in security against an individual's right to be "left alone".[40]

Hereinafter different forms of privacy intrusion through government measures will be analysed.

II.2. Closed Circuit Television (CCTV)

Mass surveillance in form of CCTV cameras is increasingly infringing individuals' rights to privacy.[41] These systems are already heavily used in the UK and have grown increasingly popular around the world. They provide for a fast, cost efficient and automated way of identifying people out of a crowd as well as behavioural pattern recognition and risk detection. New software is being developed to analyse people's movement and behaviour leading to an automated risk assessment and flagging of individual persons.[42] Thus, a nervous person being caught by the camera's software would be flagged to an officer who then has to determine the treat the person potentially poses.

One might imagine the privacy infringement when a person is going on a date to meet a love interest and being picked out by the system as potential threat. What used to be a totally private matter would now be evaluated by an individual sitting on a computer. Anonymising the stored data through encryption will not provide a solution, as decryption is possible at a later point in time.[43] Additionally, as this recording is retained, publication of such footage would infringe upon an individual's privacy in a very serious fashion. The ECHR has expressed its view that such a disclosure would go beyond the mere passer-by or security observation which can be foreseen by the individual concerned and thus would be in violation of Article 8 of the Convention.[44] However, in *Perry v. United Kingdom*[45] the Court highlighted that when the data is not recorded no human rights violation takes place.

---

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN> (accessed 10 September 2014).

40 Cooley, T. M., *A Treatise on the Law of Torts*, 2nd ed., Callaghan, Chicago, 1888, 29.

41 Vermeulen, M., and Bellanova R., "European "smart" surveillance: What's at stake for data protection, privacy and non-discrimination?", *Security and Human Rights*, vol. 23, 297–311.

42 European Commission Enterprise and Industry, Security Research: Towards a more secure society and increased industrial competitiveness – Security Research Projects under the 7th Framework Programme for Research, May 2009, 6, available online at <ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/towards-a-more-secure_en.pdf> (accessed 10 September 2014).

43 European Commission, *Article 29 Data Protection Working Party - Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, 11 February 2004, 15, available online at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf> (accessed 10 September 2014).

44 ECtHR, 28 April 2003, *Peck v. The United Kingdom*, 36 EHRR. 41.

45 ECtHR, 17 October 2003, *Perry v. The United Kingdom*, [2003] ECHR 375 [2004] 39 EHRR 3, 38.

An even stricter view has been applied in the Italian guidelines on video surveillance requiring actual, specific dangers or the suppression of concrete dangers in order to warrant video surveillance.[46]

II.3. Passenger Name Record (PNR)

The PNR system includes all personal (i.e. credit card details, meal option) data which is supplied by the passenger for booking a flight and checking in, thus essentially being collected for a commercial purpose.[47] As the EU also wants to gain the benefits of sharing this data (as currently only the US benefits from it), the Commission has proposed a new EU PNR. This would allow the tracking of certain passengers in real-time as well as retrospective pattern analysis by EU agencies. In order to carry out such, a measure a massive amount of data would need to be stored and processed. As the data is collected for commercial purposes only, it stands in stark contrast to the purpose limitation principles enshrined in EU data protection law.[48]

Additionally, the proposed retention period of up to five years is of great concern for privacy protection advocates. Despite requiring anonymisation of the data following an initial thirty-day retention period, the data would be stored for an excessively long time in light of the already growing concerns for its legality. Furthermore, the anonymisation of the data is not irreversible, as otherwise it would not be of much value anymore.[49] In particular, the government's ability to subpoena or access such commercial data creates challenges for the privacy of individuals. The longer the data is stored the higher the risk is that an unwanted disclosure could occur during its life cycle.

II.4. Public records

Government agencies, in carrying out their functions, collect a manifold amount and type of information. Such data is generally afforded some degree of protection by privacy legislation such as the Privacy Act (USA) [50] or EU country laws such as the Bundesdatenschutzgesetz in Germany. Nevertheless, these legislations differ in key aspects regarding their scope and applicability. In the USA privacy and data protection are for most parts regulated by state legislation, thus different states have a varying level of protection which also is dependent on the state constitutions. As the US Constitution only protects against the unreasonable search and seizure of information its extent is somewhat limited in situations in which private information such as a social security number or the address of a person are supplied by agency to a third party. In order to cover such a scenario one has to firstly turn to the USA Privacy Act or applicable state legislation/constitution. The District court in Michigan, for example, declined to require

---

[46] Coudert, F., "When video cameras watch and screen: Privacy implications of pattern recognition technologies", *Computer Law & Security Review*, vol. 26, 2010, 382.

[47] European Commission, Communication from the Commission on the Global Approach to Transfers of Passenger Name Record Data to Third Countries, 21 September 2010, COM (2010) 492 final, Brussels, 3.

[48] European Commission, *Article 29 Data Protection Working Party,* 08 April 2013, available online at <ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130408_pr_purpose_limitation_en.pdf> (accessed 19 August 2014).

[49] European Commission, Proposal for a Directive of the European Parliament and the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 2 February 2011, COM (2011) 32 final, Brussels, Article 9(2), 26.

[50] Section 552a Privacy Act of 1974, 5 U.S.C.

a social service to hand over the information about the location of his children to their father; he was not able to meet the requirement of showing 'compelling circumstances affecting the health or safety'[51] of his children.

In *Whalen v. Roe*,[52] the Court explained that there are two types of privacy interests that may be constitutionally protected: 'One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions'. The right to informational privacy, however, 'is not absolute; rather, it is a conditional right which may be infringed upon a showing of proper governmental interest.'[53]

What is required to allow disclosure is subject to much debate and conflicting judgments. Courts have held that where the government releases information, it must be of a highly personal nature before constitutional privacy rights will attach. In its judgment in *Eagle v. Morgan* the court noted that 'to violate [a person's] constitutional right of privacy, the information disclosed must be either a shocking degradation or an egregious humiliation.'[54]

Constitutional privacy protection extends only to 'the most intimate aspects of human affairs' and that a person's 'legitimate expectation of privacy' bears on the constitutional analysis.[55] In another decision it was held that 'mandatory disclosure of an individual's Social Security Number (SSN) to the Department of Motor Vehicles does not threaten the sanctity of individual privacy so as to require constitutional protection,' and constitutional privacy rights apply only to more personal matters such as marriage, procreation, family.[56] However, one must note that there have been a vast amount of differing decisions on the disclosure of SSN of which some allowed disclosure others prohibited it based on constitutional privacy protection.

In Europe, public agencies are bound by their individual country's laws on data protection which are mirrored according to the basis set by the EU Data Protection Directive.

III. Particular challenges in the online world

III.1. Data collection by private businesses

Growing technological capabilities have led to an imbalance between state regulation and market power of Internet enterprises. Recent enforcement action by data protection regulators has highlighted the problems associated with policing these companies. For example, Google has repeatedly violated European data protection laws by collecting wireless data acquired by their mapping cars which take pictures for Google's Street View Service. Only after increased pressure and legal action Google gave in to the German authorities and deleted the data. Furthermore, France fined Google the maximum sum of 150, 000 Euros for data protection violations in January 2014. As the maximum penalty is so low, it has been suggested that Google deliberately ignored the law calculating the fine as an expense on the way to expanding their business.

---

[51] *Roger Deplanche v. Joseph A. Califano*, Secretary of Health, Education & Welfare, individually and in his official capacity as Secretary, 549 F.Supp. 685 (1982).

[52] *Whalen v. Roe*, 429 U.S. 589 (1977).

[53] *Doe v. Attorney General of U.S.*, 941 F.2d at 796.

[54] *Eagle v. Morgan* 88 F.3d at 625 CA 8 (Ark.),1996.

[55] *Ibid*.

[56] *Stoianoff v. Commissioner of Motor Vehicles*, 107 F.Supp.2d 439 (SDNY 2000).

Another well-known entity in the context of data protection is Facebook. The social media enterprise is in constant conflict with European data protection authorities over their data protection laws because of customer surveillance. In particular the "Like" buttons enable Facebook to track user not only on Facebook but also on any site which displays such a symbol. In essence, when a user sees a "Like" button on any site he can be sure that Facebook has received his IP address, thus potentially enabling the identification of a user.[57] This is in clear violation of European data protection law as it allows Facebook to create personalised user profiles. [58] Further technological advancements such as facial recognition provide for a steady flow of new challenges for regulators in Europe.[59]

Once such data is (illegally) collected it is generally accessible through the appropriate procedures by the EU member state agencies which previously would have not had neither the capabilities nor the legislative basis to collect and process such data. Thus a potential conflict can arise when data is collected (illegally without the customer knowing or legally by way of consent through the terms of service) by a private entity for commercial purposes and subsequently used by government agencies for their legitimate public security purposes.

The right balance between privacy regulation and data protection on one side and data security on the other is hard to achieve. Without giving up some degree of privacy, data flows on the internet cannot be secured. For example, Microsoft wanted to share information with its business partners and later with the public at large on its security feed. This feed provides real time information on attacks, botnets and other treats.[60] However, such a system cannot be used under current European data protection laws as the IP addresses supplied are classed as personally identifiable information which cannot be given out to the public. Thus, in order to increase public security through alerting users to potential dangers on the Internet, such as fishing attacks, the laws need to cater for a certain degree of privacy invasion in order to achieve overall security gains.[61] Contemporary security methods mostly fall under the European Data Protection Directive's definition of personal data, thus requiring a reinterpretation or an exemption in order to improve online security.[62]

---

57 New York Times, Richmond, R., *As 'Like' Buttons Spread, So Do Facebook's Tentacles*, 27 September 2011, available online at <bits.blogs.nytimes.com/2011/09/27/as-like-buttons-spread-so-do-facebooks-tentacles/?_php=true&_type=blogs&_r=0> (accessed 19 August 2014).

58 Datenschutzzentrum, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, *Deactivate Facebook Web Analytics*, 19 August 2011, available online at <www.datenschutzzentrum.de/presse/20110819-facebook-en.htm> (accessed 19 August 2014).

59 New York Times, Griggs, M. B., *8 Weird Ways People Are Using Facial Recognition Software, Popular Mechanics*, 27 September 2011, available online at <popularmechanics.com/technology/how-to/software/8-weird-ways-people-are-using-facial-recognition-software#slide-1> (accessed 19 August 2014).

60 See Network World, Neagle, C., *Microsoft to Launch Real-Time Threat Intelligence Feed*, 12 January 2012, available online at <networkworld.com/news/2012/011212-microsoft-intelligence-254846.html> (accessed 19 August 2014).

61 See UK Ministry of Justice, Clarke, K., *Data protection: Speech by the Lord Chancellor and Secretary of State for Justice,* 26 May 2011, available online at <justice.gov.uk/news/speeches/previous-ministers-speeches/ken-clarke/260511-data-protection2> (accessed 19 August 2014).

62 Cunningham, M., "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law", *George Washington International Law Review,* vol. 44, 2012, 643–695, 688.

III.2. Old-fashioned wiretapping laws and todays internet communication

Wiretapping is a long established practice, especially in the US. During the prohibition period (1919–1933) the first cases on wiretapping emerged as police used this form of intercepting communication to identify bootleggers and their accomplices.[63] At this point in time a warrant was not required which lead to a vast amount of surveillance by the FBI over a thirty-year period. The Watergate scandal was a stepping-stone in changing public perception of surveillance and initiating legislative action limiting surveillance capabilities. Without accountability public authorities gain nearly unlimited power over the citizens of a country creating a strong imbalance between an individual's privacy rights and state powers. Putting it in the words of Benjamin Franklin: 'They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.'[64]

A couple of cases in the US have emerged that walk a fine line in balancing the competing interests of privacy and public security. For example, the well-known case of *Smith v. Maryland*[65] allowed for the collection of caller numbers through a pen registry. The court in this case was of the opinion that once a phone number was dialled and supplied to the operator it effectively lost any reasonable expectation of privacy and therefore could be accessed without a warrant by law enforcement officers. Thus, the judgment was based on the notion of publicising information rather than on a weighing of the public interest favouring disclosure.

As governments have a legitimate interest in accessing data and communication streams in certain cases, such as for crime prevention, the issue arises to what extent telecommunication and internet service providers are required to assist the authorities in accessing the information and whether they will be compensated for doing so.[66] Only after the US Congress approved 500 million USD in 1994 to cover telephone-company costs for upgrading their systems in order to be compliant with FBI requirements, did the companies drop their objection to a new surveillance law: the Communications Assistance for Law Enforcement Act (CALEA). In 2005 this law was expanded to include also voice over IP (VoIP) communications send via the Internet. After the events of 9/11 the US Patriot Act,[67] and in particular sections 214–217, expanded the surveillance powers of government agencies significantly giving them nearly unlimited access through National Security Letters and secret court subpoenas.[68]

In 2002 it came to light that the NSA had implemented secure facilities within AT&T centers which allowed them to access and reroute any communication being sent through those lines. Any calls even if purely domestic were likely to be caught by this system.

---

63 Landau, S., 'Surveillance or Security? The Risk Posed by New Wiretapping Technologies', The MIT Press, Cambridge, 2010, 67.

64 (1775) – Remarks on the Propositions (A Plan which it is believed would produce a permanent union between Great Britain and her Colonies), *in:* William Temple Franklin (ed.), *Memoirs of the life and writings of Benjamin Franklin*, vol. 1, Printed by T.S. Manning, Philadelphia, 1818, 333–334.

65 *Smith v. Maryland* 442 US 735 (1979).

66 See for example 18 USC Section 2518(4), which provides for compensation to the private entity.

67 Publ. L. No. 107 – 56: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001.

68 Jusletter IT, Weber, R. H. and Staiger, D. N., *Spannungsfelder von Datenschutz und Datenüberwachung in der Schweiz und in den USA*, 15 May 2014, available online at <jusletter-it.weblaw.ch/dms/publicationsystem/articles/jusletterit/2014/2/a1d0befe-1f4d-48bd-8e94-381dd4e3e8c8/pdf_a1d0befe-1f4d-48bd-8e94-381dd4e3e8c8> (accessed 19 August 2014).

Furthermore, in March 2004 the White House overreached its authority by simply ignoring that the Department of Justice, represented by the Attorney General, was not willing to sign off on the reauthorisation of the President's Surveillance Program (PSP) which includes warrantless wiretapping and other forms of expansive surveillance. Despite the missing approval, the White House continued the program.

Any surveillance measure requires accountability, strict oversight and enforcement procedures. Additionally, the efficiency of a surveillance regime, such as wiretapping or interception of Internet traffic, must first be determined in order to ascertain whether the measure would have any significant effects on investigation and a subsequent court trial. Practicing defence attorneys and former district attorneys have raised serious doubts as to whether the current wiretapping framework produced any evidence which would have outweighed the significant infringement upon individual privacy caused by the wiretapping.

The US government monitors all traffic to and from federal agency websites and servers. However, as a banner warns users that their traffic is monitored the government argues that there is no expectation of privacy which would prevent such measures.[69] A possible solution for users is to use a so-called Tor (The Onion Routing) system which anonymises the routing of the data sent and received. It prevents a party from identifying the receiver or sender of the data transferred on the Internet between different server and routers.[70]

New technologies such as spyware allow a public agency to access any computer system and to copy and view all data stored on it. The US government regularly requests bids for contracts on malware in order to keep up to date in the fast adapting online world.[71] Malware allows government officials to access and control a computer. As most of our daily life is spent on a computer, a large amount of personal and private information is stored and communicated through it. The use of malware therefore needs to be very strictly limited in order to be considered proportionate to the crime prevention or investigation purpose.

In Europe steps have been taken to limit the availability of data for government agencies. For example, in April 2014 the ECtHR decided that the directive regulating the storage of user identification data is not proportional to its legitimate objective and thus violates EU privacy law. This ruling will require major changes in most EU member states enabling the governments to review their data collection policies in light of the current surveillance issues.[72]

The UK Regulatory Investigatory Powers Act (RIPA) 2000 aims at regulating targeted surveillance by requiring a warrant to be issued by the Home Secretary before private communication can be intercepted, which is the prevailing method used in the European countries.

---

[69] US Department of Homeland Security, *Privacy Impact Assessment: Einstein Program,* September 2004, available online at <dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf> (accessed 19 August 2014).

[70] Tor, *Tor Project: Anonymity Online,* available online at <torproject.org/index.html.en> (accessed 19 August 2014).

[71] Federal Business Opportunities, *Malware Solicitation Number: RFQ1307A*, 12 February 2014 available online at <fbo.gov/index?s=opportunity&mode=form&id=5b4b8745e39bae3510f0ed820a08c8e2&tab=core&_cview=0> (accessed 19 August 2014).

[72] European Court of Justice, Grand Chamber, 8 April 2014, Joined cases C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and C-594/12 KärntnerLandesregierung and Others .

III.3. Open source data collection

Designing and implementing counter-terrorism measures are the main tasks of security agencies around the world. Besides using CCTV data and data provided by flight passengers, an enormous pool of open source data is available to these agencies on the Internet. According to the US Congressional Research Service around 90% of intelligence data comes from such open sources.[73] These include sources from which information can 'lawfully be obtained by request, purchase or observation.'[74]In particular social networking sites and video channels (YouTube) have become a valuable source as they allow agencies to draw a more precise picture of a person's relations and views.

This flood of data is not without risks. For example, when information is disseminated through different sources with different views the data might create a completely misplaced impression when picked up by the agencies. Nevertheless, just because the data is accessible and available does not mean that its use is ethical. Especially the risk of acquiring wrong or incomplete information which subsequently harms an innocent person must be taken into account and balanced against the detriment to be prevented in every individual case.[75]

Central to one's expectation of privacy is the environment in which information is shared. For example in a hospital setting we expect different norms to apply than in a less private and personal situation. This line is increasingly blurring as a user of a social networking site may have the reasonable expectation that only his friends can see the content he posts. In reality, however, access is granted to a much wider range of people, commercial entities and government agencies, through clauses in their Terms of Service (ToS).

Accountability for a government's use of such data is also another cornerstone in regulating government actions and their effects on individual privacy. The implications closed-door decisions have on individuals needs to be closely scrutinised. In most cases a person is not even aware that his data has been collected and thus does also not know that based on his data he was not granted a right or was denied an opportunity. Appropriate control mechanisms need to be developed in order to avoid such arbitrary decision-making behind the back of the affected parties.[76]

Even though the public's perception of a threat through terrorism or other violence generally remains high in society, this should neither justify extreme restrictions on speech and assembly, nor on procedural rights protecting individual citizens. Especially after the 9/11 event, the USA as well European countries have passed new laws limiting the rights of suspected terrorists, thus infringing on their right to privacy by allowing the ongoing monitoring of potential suspects. In particular the US Patriot Act[77] significantly expanded the surveillance powers of federal government agencies in the US. The revelations of Edward Snowden have shown the global scale of these measures.

---

[73] Open Source Intelligence (OSINT), Best, R. A. and Cumming, A., *Open Source Intelligence (OSINT): Issues for Congress*, 5 December 2007, available online at <fas.org/sgp/crs/intel/RL34270.pdf> (accessed 19 August 2014).

[74] US Office of the Director of National Intelligence, Intelligence Community Directive 301: National Open Source Enterprise, 11 July 2006, ICD 301, 8.

[75] Boyd, D., *Privacy and Publicity in the Context of Big Data*, 29 April 2010, available online at <danah.org/papers/talks/2010/WWW2010.html> (accessed 19 August 2014).

[76] Hayes, B., "Spying in a see through world: The open source intelligence industry", *Statewatch Bulletin*, vol. 1, 2010, 1-10, 2.

[77] Public Law No. 107 – 56: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001.

Efforts have been made on an international level to address the issue of profiling by state actors utilizing the new possibilities created through Big Data [78] and other technologies. In September 2013, the 35th International Conference of Data Protection and Privacy Commissioners, held in Warsaw, called upon all parties using profiling to adhere to a set list of boundaries formulated at the meeting.[79] These broad principles are intended to act as a starting point for the enactment of state legislation. They incorporate concepts such as the requirement to inform the public of the nature and extent to which profiling can be carried out in order to allow individuals to implement measures to minimise their exposure.

Furthermore, a resolution on web tracking was passed which also highlighted the issues created by mobile devices which allow for constant location tracking of its user.[80] The thereby recommended purpose limitation and information policies aim at reducing the effects of these new tracking capabilities.

III.4. Surveillance of public service employees

As an employer the government agencies have an interest in monitoring the internet and email activity of their public servants. US studies have shown that the monitoring of internet usage is a common occurrence.[81] However, such surveillance should not be undertaken lightly and only with notice to the affected individual.

The *Canadian case of Cargill Foods v. United Food and Commercial Workers International Union, Local 633*[82] highlighted that unionised employees must be giving advanced notice and meaningful discussion before an employer can increase existing surveillance. Such an impermissible surveillance includes the reading of email communication between an employee and a union official unless it is done for a legitimate objective and no other means are available to reach that objective.[83] Again, one of the cornerstones for allowing use and access to personal data by government agencies is a legitimate justification which on balance outweighs the right to privacy of the individual affected.

In determining the reasonableness of recording surveillance cameras at a workplace the following factors to be considered were established in *R. v. Oakes*[84]:

- Is the measure necessary to meet a specific need?
- Is there effectiveness in meeting that need?
- Is the loss proportional to the benefit?

---

[78] Big Data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process the data within a tolerable elapsed time. See Snijders, C., Matzat, U., and Reips, U. D., "'Big Data: Big gaps of knowledge in the field of Internet", *International Journal of Internet Science,* vol. 7, 2012, 1–5, 1–2.

[79] Privacy Commission, *Resolution on Profiling*, 26 September 2013, available at <privacycommission.be/sites/privacycommission/files/documents/Profiling-resolution.pdf> (accessed 19 August 2014).

[80] Privacy Commission, *Resolution on Web Tracking and Privacy,* 29 September2013, available online at <privacycommission.be/sites/privacycommission/files/documents/Web-tracking-Resolution.pdf> (accessed 19 August 2014).

[81] American Management Association and the ePolicy Institute, *Electronic Monitoring and Surveillance Survey*, 2008, available online at <www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf> (accessed 10 September 2014).

[82] *Cargil Foods and UFCW, Local 633 (Re)* (2008), 175 L.A.C. (4th) 213.

[83] *Universitè Laval c. Association du personnel administratif professionnel de l'Universitè Laval*, 2011 CanLII 6949 (QC SAT).

[84] *R. v Oakes*, [1986] 1 S.C.R. 103.

- Is there a less privacy-invasive method of achieving the same result?

In 2004 these factors were reaffirmed highlighting that the CCTV footage could not be used for another purpose than it had been collected for, which in this case was for security purposes.[85] Thus, as a productivity measuring tool, such camera evidence is not available.

III.5. Use of public data by private corporations

Recently a Swedish startup company (Lexbase) started offering information on private individuals' criminal and civil suits on an open Internet database. In Sweden this is possible as the Constitution provides for extensive public access to government data, even if it concerns a private individual.[86] Such an approach to public disclosure and privacy can have significant effects on a vast amount of individuals. It stands in contrast to the generally accepted balancing of interests of the parties involved.

When such a gatekeeper function to access personal information is lost then the information is open to abuse by various parties, which in combination with new technologies can create individual profiles of people. The effect of such profiling should not be underestimated. When personal data is so easily accessible this might be a deterrent to access the court system for smaller claims as one might not want to make smaller disputes public by having a record at the courthouse. Thus, a system that is open and transparent and wants to provide a secure reliable public service might sabotage its own goals through excessive transparency in private matters.

Additionally, the right to be forgotten is relevant in this regard, as public data which is obtained by a private corporation should be deleted once the data is not available on the public system anymore.[87] Such an approach is necessary to preserve an individual's privacy rights. This view has been supported by a recent European Court of Justice decision on the storing of a foreclosure reference in a Google search.[88] The Court was of the opinion that the individual subject to the foreclosure has the right to have the reference deleted from the automatic search enquiry field Google provides. However, any such privacy right will need to be balanced against the public interest of its disclosure. Thus, over time the balance shifts towards the privacy interest of the individual requiring the deletion of the data at some later point. Nevertheless, it is also possible that the public interest in deleted data can once again outweigh the privacy rights of an individual, for example when a person runs for a public office and it is in the public interest to know previously deleted information as to his criminal history.

---

85 *Eastmond v. Canadian Pacific Railway,* 2004 FC 852 (CanLII), para 174, 176&177.

86 Chapter 2(1) The Freedom of the Press Act, Sweden, 1949 as in force on 1 January 1999, available online at <riksdagen.se/Global/dokument/dokument/laws/the-freedom-of-the-press-act-2012.pdf> (accessed 10 September 2014): 'Every Swedish citizen shall be entitled to have free access to official documents, in order to encourage the free exchange of opinion and the availability of comprehensive information'.

87 For a detailed discussion see Sartor, G., "The right to be forgotten: Publicity, privacy and the passage of time", *in*: Schartum, D.W., Bygrave, L. and Bekken, A.G., eds., *Jon Bing – A Tribute*, Glydendal Akademisk, Oslo, 2014, 79–102.

88 ECJ, 13 May 2014, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, available online at <curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11654> (accessed 10 September 2014).

III.6. Finding the fine line of disclosure

In practice often challenging scenarios arise when data is collected by a government agency, such as, for example, the criminal record of a public service employee. During the course of the data storage period frequent access requests to this data can be made from within the agency storing the data, other unrelated governmental entities, and private sector actors as well as courts.

In a 2011 Canadian case a public agency disclosed a public service employee's personal record during a pre-trial discovery process which was found to be in violation of that person's privacy interest.[89] The disclosure was not required under the law and was carried out voluntarily without the employee's consent. It violated the legitimate privacy expectations of the employee as a later disclosure could have been carried out without harm. Therefore, the element of objective justification was missing.

It seems that disclosure of personal information as well as any processing or use by government entities must be subject to a balancing act. This should include the reasons for disclosure, use or access as well as the means and potential alternatives to such means. Additionally, the potential harm to the individual should also be taken into account and contrasted to the effect non-disclosure, use or processing would have on the legitimate interests of the public agency in question.

IV. Outlook on the future of privacy regulation

IV.1. Current developments in international efforts

The last couple of years have shown a strong shift in privacy awareness and regulation all around the globe. For example Australia utilises so called Privacy Protection Principles[90] which provide the boundaries for data use and attract substantial fines when breached.[91] Technological progress further increases the need for reform in the privacy and data protection environment. This is evidenced by the reform steps undertaken in Europe with the proposal for a new Data Protection Regulation as well as the US surveillance reform agenda. Despite these encouraging signs of a new awareness, the law is currently not able to keep up with new technologies.

Increasingly the US has come under pressure to rethink and reform its surveillance framework in light of the Snowden revelations. Most important in achieving a balanced approach to the competing interests of privacy and public security is the definition of clear principles on the competences of the state and in what circumstances privacy infringements will be tolerated. Any such measure must be reviewable by a court in a proceeding in which the affected party is heard.

The EU has addressed the issue of privacy through its Data Protection Directive[92] which will soon be superseded by a new Regulation. The Directive does not apply to the

---

89 Ontario Public Service Employees Union (Union) v. Ontario (Government Services), 2011 CanLII 23158 (ON GSB).

90 Schedule 1 Privacy Act, Australia, 1988 as in force on 12 March 2014, available online at <comlaw.gov.au/Details/C2014C00076> (accessed 10 September 2014).

91 *Id.*, Section 13(1).

92 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available online at <eur-

processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union, nor, in any case, to processing operations concerning public security, defense, state security or the activities of the state in area of criminal law.[93] Additionally, a basic framework for the processing of personal data by public authorities is currently being proposed. [94] In its Framework Decision 2008/977/JHA the European Council acknowledged that the existing data protection instruments at the European level do not suffice.

IV.2. Balancing of competing interests

Limiting a government's ability to infringe a citizen's privacy to existing and established methods which have proven to be least invasive and successful in reaching their predetermined objective appears to be a sensible approach to the situation at hand. Before engaging in the use of more invasive technologies such as the open source data collection, in combination with big data technologies in order to identify individuals and their behavioural patterns, a concrete balancing exercise must be carried out. This should include the evaluation of the potential risks to society which are to be prevented, the likelihood of their occurrence, the probability of preventing them through the measure to be implemented as well as the effects the measure has on the individual's privacy rights and society at large.[95] In Europe this balance is struck by placing a focus on the rights of the individual and the effects created by the disclosure or use of his personal data.[96] Such a right will be infringed if his data is not processed in accordance with basic data protection principles. However, the right is not absolute and yields to important concerns such as the securing of democracy.[97] Importantly, the approach taken by the ECHR when determining whether a privacy invasion is necessary is a very strict one.

In contrast to a weighing of broader social benefits the US Supreme Court has only recognised a very basic form of informational autonomy and stronger independence only in making certain kinds of important decisions.[98] Interestingly, the US draws a distinction between the types of interest and places a lesser protection on individual's decisions when they fall into the private sphere. [99] The Fourth Amendment of the US Constitution requires for its protection to apply a reasonable expectation of privacy which does not

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (accessed 10 September 2014).

93 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, point 5, available online at <eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN> (accessed 10 September 2014).

94 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, available online at <eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=en> (accessed 10 September 2014).

95 Power, M., *The Law of Privacy*, Lexis Nexis Canada, Ontario, 2013, 33–44.

96 BVerfGE 65, 1(48).

97 BVerfGE 65, 1(43).

98 *Whalen v. Roe*, 429 US 589 (1977), 598.

99 *Roe v. Wade*, 410 U.S. 113 (1973).

include things that occur in the public space.[100] This interpretation has led to a narrow application of the provision. As the law currently stands in the US a compelling interest is required in order to justify the invasion of privacy by limiting a person's right to decide on private matters.[101] The standard to determine whether a legislative enactment impermissibly infringes on the state constitutional right of privacy places the burden of proof on the state to justify an intrusion on privacy; the burden can be met by demonstrating that the challenged regulation serves a compelling state interest and accomplishes its goal through the use of the least intrusive means.[102] As expressed in a Californian judgment 'while the legislative investigatory power is broad, it must satisfy constitutional and applicable legal standards'.[103]

Limiting the purpose for which a government agency can use data which infringes on an individual's privacy is essential. In this regard the Australian High Court has held that data collected under a statute for a specific purpose can only be used for that purpose and requires consent by the data subject for any other use.[104] This approach goes beyond what was previously required under the Australian federal Privacy Act, thus it appears that the courts have realised the need for further boundaries in regard to privacy and have send a signal to the legislator to react to the changing technological environment.

The approach to balancing competing interests of the individual to personal privacy and a state's interest in security varies throughout the common as well as civil law jurisdictions. For example in most Canadian jurisdictions the use or disclosure of data must have a reasonable and direct connection to the original purpose and its disclosure must be necessary to the performance of a statutory duty.[105] Furthermore, most Canadian statutes relating to data protection include a concept of unreasonable invasion of privacy[106] which assists in determining whether a government agency should disclose personal information.

In order to allow an aggrieved party to enforce its privacy rights the applicable state legislation should also define with reference to specific elements under which circumstances an invasion of privacy occurs.[107] Such a framework would reduce the current hurdle for private individuals to ascertain objectively whether they can be successful in a cause of action against state agencies, thus lowering the bar to claiming their respective rights. This includes the need for a right to access information stored by government agencies which should not limit its scope by imposing undue requirements such as citizenship upon a requesting party.

Discretionary exemptions allow an agency to determine whether the information is of such a nature that it would harm broader state interests and thus on balance should not

---

[100] Gellman, R., "A General Survey of Video Surveillance Law in the United States", *in:* Nouwt, S., de Vries, B. R. and Prins, C., eds., *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy,* T.M.C. Asser Press, The Hague, 2005, 7–35.

[101] *American Academy of Pediatrics v. Lungren*, 32 Cal.Rptr.2d 546 (Ct. App 1994).

[102] *North Florida Women's Health And Counseling Services, Inc., et al. v. State of Florida, et al.* 866 So.2d 612 (Fla. 2003).

[103] *Connecticut Indemnity Company et al., v. City of Lodi*; *Maryland Casualty Company et al. v. City of Lodi*, 86 Cal.Rptr.2d 515 (Cal. App 1999).

[104] *Johns v. Australian Securities Commission and Others* (1993) 178 CLR 408.

[105] Power, *supra* nt. 95, 37.

[106] Section 43 Freedom of Information and Protection of Privacy Act, Ontario, 1990 as in force on September 12 2014, available online at <e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm#BK57> (accessed 10 September 2014).

[107] Most Canadian privacy laws include such an illustration of situations were a breach has occurred.

be disclosed. Enabling a speedy review of such a decision by a competent court or ideally as a first step by an Information Commissioner must be part of this exemption.[108] Effective sanctions in form of penalties which act as a deterrence for public officials to breach the privacy of individuals contrary to law are also central to a complete privacy protection framework.

*

www.grojil.org

[108] Power, *supra* nt. 95, 171.

Privacy as an International Human Right and the Right to Obscurity in Cyberspace

Alexandra Rengel*

Keywords
RIGHT TO PRIVACY; HUMAN RIGHTS; RIGHT OF OBSCURITY; PRIVACY BY DESIGN; PERSONAL DATA; CYBERSPACE; INTERNET

Abstract
Fundamental rights are considered to be those which human beings have by the fact of being human and are neither created nor can be abrogated by any government absent extraordinary circumstances. They are fundamental in that the enjoyment of such rights is necessary to live a life with dignity. Fundamental rights are recognized by several international conventions and treaties such as the International Convention on Civil and Political Rights, and the International Convention on Economic and Social Rights and they include cultural, economic, and political rights, such as the right to life, the right to liberty, the right of association, and the right to freedom of religion. Privacy is an essential human need. Although the concept of privacy has a certain abstract quality to it that makes it difficult to define, instinctively, humans need to know that they can keep some things secret from others. Absent extraordinary circumstances the need for humans to have a certain degree of privacy is innate. Perhaps as a result of that intrinsic need, privacy as a concept has been recognized in a social as well as a legal sense in most cultures from time immemorial. Today, the right to privacy is considered to be an identifiable human right with universal qualities deserving legal recognition and protection, although the scope of such legal protection is still being determined.

In reviewing the concept of privacy, new technologies often make us wonder what level of protection of our right to privacy is possible in a world where personal information about us can be accessed not by infringing our physical space, but by invisible hands that can access our most private secrets just by pressing a button and looking at a screen. New technologies in the form of the Internet, social networks, remote access to information, etc., make it increasingly more difficult to maintain privacy rights in cyberspace such that online invisibility has become impossible. The quest for invisibility is the idea that individuals should be able to choose to remain invisible online. In order for that scenario to become a reality more emphasis needs to be made on the universal recognition of privacy principles in the context of cyberspace. Additionally, design based privacy solutions must be created to protect individuals' privacy in cyberspace.

---

* Alexandra I. Rengel is the author of *Privacy in the 21st Century*, Martinus Nijhof Publishers. She is an attorney in private practice in the firm of Mercado & Rengel. Ms. Rengel received her B.A. from Mount Holyoke College and earned her JD from Boston University School of Law. Ms. Rengel is a *summa cum laude*, valedictorian graduate of the St. Thomas University School of Law LLM. Program in Intercultural Human Rights. She also obtained her JSD at St. Thomas University School of Law, writing her dissertation on the right to privacy in the international context, for which she was distinguished with *summa cum laude* honors. Ms. Rengel teaches at Suffolk University, Madrid campus; at Comillas Pontifical University in Madrid; and at the Instituto de Empresa in Madrid. She is also a frequent lecturer on human rights, international business law and arbitration. Ms. Rengel writes this article with special thanks to her husband, Ivan Mercado and her children Maria and Ivan.

I. The Law of Nations and Fundamental Human Rights

Before the Roman Empire, religion served as the paramount source of the law of nations.[1] During the Middle Ages, international, or universal, law merged with ecclesiastical law, and even treaty law was considered to have legal force only because treaties were confirmed by oath, which, being a "sacrament," subjected the obligation incurred to the jurisdiction of the Church.[2] Medieval legal scholars did not distinguish municipal from international law, instead viewing the law of nations as a universal law, binding upon all mankind.[3] Thus, in these early years, the public/private, domestic/international categories that later came to dominate classical international legal theory had not been developed, and were, in practice, unnecessary. The law of nations was thought to embrace private as well as public, domestic, as well as transborder, transactions, and to encompass not simply the "law of states," such as rules relating to passports and ambassadors, but also the law between states and individuals, including the "law maritime" (affecting shipwrecks, admiralty, prizes and the like) and the "law merchant" (*lex mercatoria*), applicable to transnational commercial transactions.[4] Throughout the eighteenth century, an increasing interdependence and interaction between nations called for a more uniform system of laws. Under the modern framework of international system of laws adopted, the scope of authority possessed by international organisations depends almost entirely upon the constitutional limitations in their charters as well as a nation's express consent to submit to the authority of those international organisations.[5] However, over time, international law has also benefitted from the

---

1 See generally Bederman, D. J., "Religion and the Sources of International Law in Antiquity", *in:* Janis, M. W. and Evans, C., eds., *The Influence of Religion on the Development of International Law*, Martinus Nijhoff Publishers, The Hague. 1999, (In his article, Bederman traces the role of religion in the Near East during the empires of Egypt, Babylon, Assyria, Hittites, Mittani, Israelites, Greek city-states, Indian states before 150 BC, and Mediterranean powers before 168 BC).

2 Nussbaum, A., *A Concise History of the Law of Nations*, Macmillan Co., New York, 1947, 58–59.

3 Dickinson, E. D., "The Law of Nations as Part of the National Law of the United States", *University of Pennsylvania Law Review*, vol. 101, ed. 1, 1952, 26–27.

4 Berman, H. J. and Kaufman, C., "The Law of International Commercial Transactions (Lex Mercatoria)", *Harvard International Law Journal*, vol. 19, ed. 1, 1978, 224–229 (explaining that law merchant was transnational private law based not on any single national law but on mercantile customs generally accepted by trading nations).

5 See United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS 16, Articles 1–2 (detailing purposes of the UN and limits on the UN's international authority); Statute of the International Court of Justice, June 26 1945, 33 UNTS 993, Articles 34–38 (limiting competence of ICJ). The Charter of the United Nations declares itself to be an embodiment of positive law. See *ibid* (outlining the purposes and limits of the UN). The Charter states that its intent is to 'establish an international organization to be known as the United Nations', see UN Charter preamble, and specifically limits its membership to 'all other peace-loving States which accept the obligations' of the Charter. See UN Charter Article 4 (discussing the intent of UN Charter).
The UN Charter also constitutionally limits the scope of the organisation's function and purpose. UN Charter Articles 1–2. The Charter indicates that its purposes and principles are:

> 1. To maintain international peace and security; ...
> 2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;
> 3. To achieve international co-operation in solving international problems of an economic, social, cultural or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

recognition of international custom as a source of law. The law of nations includes the Statute of the International Court of Justice (ICJ); [6] Article 38 of the Statute of the International Court of Justice lists the sources of international law and includes what is known as "customary international law." [7] Customary international law has equal authority with conventional laws, such as treaty law, and is relied upon for its important role in providing a rule of law in areas of international law in which there is no applicable conventional rule. Customary international law receives the status of "law" because the ICJ considers custom as 'evidence of a general practice accepted as law' and thus as 'part of the corpus of general international law.'[8] International customary law consists of the general practices or rules of behaviour that states observe and follow out of a sense of self-perceived legal obligation.[9] There is no minimum number of adhering states required to meet the generality requirement. The United States Supreme Court in *The Paquete Habana* case[10] and the Permanent Court of International Justice in The Case of the S.S. Wimbledon[11] and *The S.S. Lotus* case[12] deduced rules of customary international law from the practice of fewer than a dozen states.[13] Customary law gains decision-making value through state practice, which eventually develops into a legal norm through persistent use and final acceptance by domestic and international jurists and commentators.[14] In the context of human rights, the notion that there is a "higher" type of law that can be

---

4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.

Ibid. Article 1 (discussing the intent of the UN Charter).

Further, the UN Charter expressly limits the ability of the United Nations to act in international matters without the express consent of the involved nations:

1. The Organization is based on the principle of the sovereign equality of all its Members.
7. Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any State or shall require the Members to submit such matters to settlement under the present Charter; ...

Id. Article 2 (discussing limitations on UN's authority to act in international matters).

6 Statute of the International Court of Justice, June 26 1945, 33 UNTS, 993.

7 *Id.*, Article 38(1)(b).

8 *Id.,* Article 38(1)(b); International Court of Justice, *North Sea Continental Shelf*, Judgment of 20 February 1969, ICJ Reports, 3, 28.

9 Restatement of the Law Third: The Foreign Relations Law of the United States, American Law Institute Publishers, 1987, Article 102.

10 The United States Supreme Court, 8 January 1900, *The Paquete Habana*, 175 US 677, (1900), 707–708.

11 Permanent Court of International Justice, *Case of the S.S. Wimbledon*, Judgment of 17 August 1923, PCIJ (ser. A) No. 1, 15, 25 and 28. In this case, the Court cited only the Suez Canal and Panama Canal regimes as "precedents" for the rule involving the Kiel Canal.

12 Permanent Court of International Justice, *The Case of the S.S. Lotus*, Judgment, of 7 September, PCIJ (ser. A) No. 10 1927, 4 and 29. The Court cited, as decisive precedents, cases involving only five states: France, Italy, Great Britain, Germany, and Belgium. On 2 August 1926 there was a collision between the S.S. Lotus, a French steamship (or steamer), and the S.S. Boz-Kourt, a Turkish steamer, in a region just north of Mytilene. As a result of the accident, eight Turkish nationals aboard the Boz-Kourt drowned when the vessel was torn apart by the Lotus. The main issue in the Lotus case was jurisdiction. The issue at stake was Turkey's jurisdiction to try Monsieur Demons, the French officer on watch duty at the time of the collision.

13 Some scholars have argued for the rule of generality to be relaxed. For example, D'Amato rejects the view that there must exist "broad participation" of states in the creation of the rule to be consistent with principles of customary international law. His standard for a valid claim based on a rule of customary law would require only that an 'objective claim of international legality be articulated in advance of, or concurrently with, an act which will constitute the quantitative elements of custom.' D'Amato, A., *International Law: Process and Prospect*, Cornell University Press, New York, 1971, 191–192.

14 Simma, B. and Alston, P., "The Sources of Human Rights Law: Custom, Jus Cogens, and General Principles", *in:* Alston, P., ed., *Human Rights Law,* New York University Press, New York, 1996*,* 3–8.

enforced internationally without the express consent of the sovereign is well recognised. Based partly on treaty law as well as customary international law, human rights law provides a set of universal standards that transcend particular cultural and historical circumstances, making it possible for trained observers to judge the conduct of both individuals and nations.[15] International human rights law attempts to adapt the practices of local cultures in order to bring them in line with certain universal principles of human rights.[16] As such, international human rights law is based on the idea that there are universal standards of human rights that supersede local and cultural customs that are not necessary to life itself, but which are considered necessary for human beings to live a dignified life. The Universal Declaration of Human Rights, which was the first document to enumerate a list of rights, represents the ideal that there are certain rights that ought to be universally protected.[17]

The Universal Declaration of Human Rights was not meant to impose legal obligations on states at the time of its adoption by the General Assembly in 1948. The status of the Declaration as described by the United Nations was that of 'a manifesto with primarily moral authority,' the first of four stages in the generation of the documents the General Assembly has collectively called the International Bill of Human Rights.[18] In contrast to the more political or hortatory Declaration, the subsequent three documents: the International Covenant on Civil and Political Rights, its Optional Protocol, and the International Covenant on Economic, Social and Cultural Rights were consciously adopted as legally binding treaties open for ratification or accession by states.[19]

Subsequent to the ratification of what is called the International Bill of Rights, international human rights law has continued its development. The creation of international tribunals, which are capable of judging the conduct of states, and even individuals, who might have committed human rights violations, was possible because of a belief that there were certain basic principles that could be universally recognised despite variations in cultures and customs around the world, and despite the lack of a universal legislative body creating a set of laws applicable to all.[20] Today, it is well established that there are certain human rights that are fundamental to human dignity and must be legally protected by all nations.[21]

---

[15] Stanlis, P. J., *Edmund Burke and the Natural Law*, University of Michigan Press, Michigan, 1958, 7: ´Natural Law was an eternal, unchangeable, and universal ethical norm or standard, whose validity was independent of man's will; therefore, at all times, in all circumstances and everywhere it bound all individuals, races, nations, and governments.´); Verdross, A., "Jus Dispositivum and Jus Cogens in International Law", *American Journal of International Law*, vol. 60, ed. 1, 1966, 55.

[16] Koh, H. H., "How is International Human Rights Law Enforced?", *Indiana Law Journal,* vol. 74, ed. 4, 1999, 1416–1417.

[17] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

[18] The four instruments referred to as the International Bill of Human Rights are as follows: Universal Declaration of Human Rights; The Charter of the United Nations; The International Covenant on Civil and Political Rights, 16 December 1966, 171 UNTS 999; The International Covenant on Economic Social and Cultural Rights, 16 December 1966, 3 UNTS 933.

[19] *Ibid*.

[20] Such claims attached in particular to influential United Nations Documents such as the Universal Declaration of Human Rights, *supra* nt. 17.

[21] For a critique of the "universalist" and "relativist" views of human rights see generally Weston, B.H., *"*Human Rights and Nation-Building in Cross-Cultural Settings", *Maine Law Review*, vol. 60, ed. 2, 2008, 318, Professor Weston concludes as follows

> In any event, one thing is certain: if one is to take seriously the proposition that respect is "the core value of all human rights," there is no escaping that cross-cultural decision-making about relativist-universalist controversies cannot be a simpleminded affair. Necessarily, it must reflect the complexity of life itself, implicating a whole series of interrelated activities

II. Privacy as a Fundamental Human Right

References to the concept of individual privacy have been prevalent since the inception of civilisation. The concept of privacy is mentioned in the Code of Hammurabi,[22] the Bible,[23] the Qur'an,[24] Jewish law,[25] and was present in classical Greece and ancient China.[26] The need for privacy is not limited to certain cultures, and most societies regard some areas of human activity as being unsuitable for general observation and knowledge.[27] However, despite the recognition of the need for privacy in the abstract, providing a concrete definition of the notion has eluded social scientists, jurists, philosophers, and others seeking singular clarity on the subject.[28] Robert Post stated that: '[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.'[29] Arthur Miller declared that privacy is 'difficult to define because it is exasperatingly vague and evanescent.'[30]

The basic need for privacy at a personal level and for society as a whole also translates into the expectation that our governments will protect our privacy from unwanted

---

and events that are indispensable to effective inquiry and therefore to rational and respectful choice in decision.

[22] The Code of Hammurabi is a Babylonian law code dating back to about 1772 BC which details a set of principles meant to guide citizens of Babylonia with various activities such as agriculture, commerce, land rights, and contractual agreements. Article 21 of the Code of Hammurabi states: '[i]f a man makes a breach into a house, one shall kill him in front of the breach and bury him in it.' Article 21, *Code of Hammurabi*, 1750–1700 BC as quoted *in:* Lasson, N. B., *The History of the Development of the Fourth Amendment to the United States´ Constitution*, John Hopkins Press, Baltimore, 1937, 14–15.

[23] Hixson, R., *Privacy in a Public Society: Human Rights in Conflict*, Oxford University Press, New York, 1987, 3; Moore, B., *Privacy: Studies in Social and Cultural History*, Random House, New York, 1984.

[24] *Sahih Bukhari*, Volume 1, Book 10, Number 509; *Sahih Muslim*, Book 020, Number 4727; *Sunan Abu Dawud*, Book 31, Number 4003.

[25] Rosen, J., *The Unwanted Gaze: The Destruction of Privacy in America*, Random House, New York, 2000, 16.

[26] Moore, *supra* nt. 23; Jingchun, C., "Protecting the Right to Privacy in China", *VUW Law Review*, vol. 36, ed. 3, 2005, 646–647 (the author states that privacy was protected, to some extent, in ancient China and an awareness of privacy may be found in the Warring States Period, referring to the era of about 475 BC to 221 BC).

[27] Mead, M., *Coming of Age in Samoa: A Psychological Study of Primitive Youth for Western Civilization*, American Museum of Natural History, New York, 1973, 219. (Margaret Mead studies of Samoan culture which revealed that children were raised by village members and exposed to all aspects of life in the public arena).

[28] See, e.g., Young, J. B., "Introduction" *in:* Young, J. B., ed., *Privacy 2,* 1978: '[P]rivacy, like an elephant, is perhaps more readily recognized than described.'; Krotoszynski, R.J., "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law*", Duke Law Journal*, vol. 1990, ed. 6, 1398–1454, 1401.

[29] Post, R. C., "Three Concepts of Privacy*"*, *Georgetown Law Journal*, vol. 89, ed. 6, 2001, 2087–2098, 2087.

[30] Miller, A. R., *The Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, Michigan, 1971, 25; see also Gormley, K., "One Hundred Years of Privacy", *Wisconsin Law Review*, vol. 1992, ed. 5, 1992, 1335, 1339: '[L]egal privacy consists of four or five different species of legal rights which are quite distinct from each other and thus incapable of a single definition.'; Mc Carthy, J. T., *Rights of Publicity and Privacy*, Clark Boardman Callaghan, New York, 1999, section 5:59: 'It is apparent that the word "privacy" has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts .... Like the emotive word "freedom", "privacy" means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.'; Gross, H., "The Concept of Privacy*"*, *New York University Law Review*, vol. 42, ed. 1, 1967, 34, 34–35: 'stating that, we can readily recognise a threat to privacy 'yet stumble when trying to make clear what privacy is'.

intrusions. However, in order to determine the behaviours that cause a breach of the right to privacy and what level of protection is warranted, it is essential to clarify what the term privacy means, and to distinguish between the concept of privacy and the right to privacy.[31] The concept of privacy involves a definition of what it entails as well as how is it valued, while the right to privacy refers to the recognition that privacy should be legally protected. It is understood, however, that the concept of privacy and the right to privacy are intertwined, because without a definition of privacy, or at a minimum, a concrete way to conceptualise privacy, it would be impossible to formulate the appropriate legal framework for the protection of the right to privacy.

As for those who have attempted to provide an all-encompassing working definition of privacy, the definitions are varied. Privacy has been defined in the context of personal autonomy or control over the intimacies of personal identity.[32] Some define privacy as focusing on control over information about oneself. [33] Alan Westin described privacy as a 'claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'. [34] According to Hyman Gross, 'privacy is the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited'.[35] Philosopher Sissela Bok states that 'privacy is the condition of being protected from unwanted access by others – physical access, personal information, or attention'.[36] Daniel Solove, after studying the concept of privacy in great depth, has classified the different conceptions of privacy into six general types: (1) the right to be let alone; (2) limited access to the self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of certain matters from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one's personality, individuality, and dignity; and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life.[37] Although there is clearly an overlap of the different conceptions, this classification reflects the various theories on privacy. After examining the six categories, Solove finds that if the purpose of conceptualising privacy is to define its unique characteristics, the classifications fall short of achieving that task because they are either too narrow, thereby failing to include some aspects of life generally viewed as private, or too broad and fail to exclude matters not generally viewed as private.[38] Solove's own theory of privacy is that

> The value of privacy must be determined on the basis of its importance to society, not in terms of individual rights. Moreover, privacy does not have a universal value that is the same across all contexts. The value of privacy

---

[31] Solove, D. J., "Conceptualizing Privacy", *California Law Review*, vol. 90, ed. 4, 2002, 1087–1156, 1088.

[32] Gerety, T., "Redefining Privacy", *Harvard Civil Rights-Civil Liberties Law Review*, vol. 12, ed. 2, 1977, 236.

[33] Parent, W., "Privacy, Morality and the Law", *Philosophy and Public Affairs*, vol. 12, ed. 4, 1983, 323–333.

[34] Westin, A. F., *Privacy and Freedom*, Atheneum, New York, 1970, 330–364. The author further explained that: '[v]iewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy, or, when among larger groups, in a condition of anonymity or reserve.

[35] Gross, *supra* nt. 30, 35–36.

[36] Bok, S., *Secrets: On the Ethics of Concealment and Revelation*, Pantheon, New York, 1983, 10–11.

[37] Solove, D., *Understanding Privacy*, Harvard University Press, Cambridge, 2009, 13.

[38] *Ibid.*

> in a particular context depends upon the social importance of the activities that it facilitates.[39]

In effect, Solove contends that we should explore what privacy means for individuals by looking at real privacy problems. He advances a pragmatic approach to conceptualising privacy, by looking at how practices involving privacy have changed throughout history and by advocating a contextual analysis of privacy.[40]

As a right, privacy has been defined as the general 'right to be left alone',[41] and a 'generic term encompassing various rights recognized ... to be inherent in the concept of ordered liberty.'[42] The right to privacy is related to the right to secrecy, to limiting the knowledge of others about oneself.[43] As such, the right to privacy could be described as the right to keep a sphere of our lives away from government intrusion, and away from the intrusion of others with whom we do not want to share certain aspects of our lives. In that sense, the right to privacy would mean a myriad of different things such as, control over personal information, freedom from surveillance, protection from invasions into one's home, personal autonomy, control over one's body and a series of other things.[44]

Some scholars have argued that the right to privacy is a necessary requirement for life in modern democratic society.[45] Political scientist Priscilla Regan states that privacy interests are not individual interests but the interests of society. She explains how individual perceptions fail to appreciate the importance of privacy for individuals fails to recognise its importance as common, public and collective values. According to Regan, '[m]ost privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but common, public, and collective purposes.'[46] In the abstract, the moral value placed on the concept of privacy varies. Most argue that privacy as a concept is an intrinsic good,[47] and that privacy is closely implicated in the notions of respect for others and oneself, as well as love, friendship and trust.[48] Jeffrey Reiman states that privacy functions 'as a means of protecting freedom, moral personality, and a rich and critical inner life.'[49] Edward Bloustein wrote that privacy is an interest of human personality, and to protect an individual's privacy is to protect the individual's

---

[39] *Id.* 39–77.

[40] *Ibid.*

[41] See S. Warren and L. Brandeis, "The right to Privacy"*, Harvard Law Review* vol, 4, ed. 5, 1890, 193.

[42] US Supreme Court, *Katz v. U. S.*, 389 US 347, at 350 (1967*);* Texas Supreme Court, *Industrial Foundation of the South v. Texas Industrial Accident Board*, 540 SW 2d 668, 679(1976).

[43] Cavoukian, A. and Tapscott, D., *Who Knows: Safeguarding Your Privacy in a Networked World,* McGraw-Hill, New York, 1997.

[44] See Newell, P. B., "Perspectives on Privacy", *Journal of Environmental Psycholo*gy, vol. 15, ed. 2, 1995, 87–105. In this comprehensive review of literature, published in 1995, psychologist Patricia Brierley Newell identified at least seventeen discrete concepts of privacy. These included describing privacy as a phenomenal state or condition of the person, a quality of place, a space of refuge, a goal, a descriptor of personal space or territoriality, a level of close personal intimacy, a behaviour, a process, a legal right, a descriptor of an interactive condition (such as an attitude, solitude, anonymity, and secrecy) and the ability to control information, among others.

[45] Westin, A. F., *Privacy and Freedom*, The Bodley Head Ltd, London, 1970, 330–364.

[46] Regan, P., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, 1995.

[47] Schoeman, F. D., "Privacy and Intimate Information"*, in:* Schoeman, F.D., ed., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge, 1984, 403.

[48] Fried, C., "Privacy", *Yale Law Journal*, vol. 33, ed. 3, 1968, 475–493.

[49] Reiman, J., "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future", *Santa Clara High Tech. Law Journal*, vol. 11, ed. 1, 1995, 27–44.

personality, independence, dignity and integrity.[50] Others defend it as a broader concept necessary for the development of varied and meaningful relationships.[51] Thus, privacy can be viewed not only as a personal value intrinsically beneficial to preserving our sense of self, but also an essential value for society.

The right to privacy has been long recognised by the international community. A review of the basic international conventions of international human rights reveals that privacy is mentioned in most of them.[52] Pursuant to article 28 of the International Covenant on Civil and Political Rights, (ICCPR), a committee of 18 independent experts, known as the Human Rights Committee, was formed to oversee implementation of the ICCPR within the States Parties to that treaty.[53] Although, the text of the ICCPR is ambiguous about what is intended by the "general comments". According to article 40(4), the Human Rights Committee may issue "general comments," to be distributed to States Parties and which are deemed to be "authoritative interpretations" of the relevant part(s) of the ICCPR that the particular comments address.[54] The Human Rights Committee issued a General Comment on article 17 of the ICCPR, which embodies the right to privacy, discussing and clarifying concepts such as: "arbitrary interference", "family", "home" and "correspondence".[55] The General Comment sheds light on how the ICCPR should interpret the right to privacy within the realm of international law.[56] According to the Human Rights Committee, the term "unlawful" as it appears in Article 17 explains that no one's privacy must be interfered with unless reasoned by law.[57] In the event that an intrusion into a person's privacy is necessary '[t]he competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant.'[58] The gathering of personal information is also addressed in the General Comment providing that law must regulate such collection.[59] Likewise, states

---

50 Bloustein, E., "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", *New York University Law Review*, vol. 39, 1964, 962–1007, 971.

51 Gerstein, R. S., "Intimacy and Privacy", *Ethics,* vol. 89, ed. 1, 1978, 76–81; Innes, J., *Privacy, Intimacy and Isolation*, Oxford University Press, New York, 1992.

52 The main human rights instruments are as follow: Universal Declaration of Human Rights, Article 12; International Covenant on Civil Political Rights, Article 17 (1966); UN International Covenant on Economic Social and Cultural Rights, Article 11; UN International Convention on the Elimination of All Forms of Racial Discrimination, 660 UNTS 195 (1969), Article 5; International Conference of American States, The American Declaration of the Rights and Duties of Man, 9th Sess., UN Doc. E/CN.4/122 (1948), Article 9; Organization of American States, American Convention on Human Rights "Pact of San Jose, Costa Rica" (B-32), 22 January 1969, Article 11; Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, Article 8; Organization of the African Union, The African Charter on Human and People's Rights, Doc. CAB/LEG/67/3/Rev.5 (1981), 5, 21 ILM 58 (1982).

53 *Id.*, Article 28.

54 *Ibid.*

55 GA Report of the Human Rights Committee (43rd session) A/43/40, 1988.

56 *Id.*, para. 1. Here it states the following: 'Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.'

57 *Id.,* para. 3.

58 *Id.*, para. 7.

59 *Id.*, para. 10.

are under an obligation to provide adequate legislation for the protection of personal honour and reputation.[60] The General Comment also clarifies that under Article 17 of the ICCPR that privacy rights are not absolute.[61] In addition to the General Comment, the European Convention of Human Rights and the Universal Declaration of Human Rights limit the scope of protection, recognising offsetting interests to which the right to privacy must yield.[62] Thus, states may lawfully restrict an individual's rights in order to protect the rights of others, the general welfare, public order, morality and the security of all.[63] However, these restrictions may not result in rendering the right a nullity.

Gradually, the right to privacy has become universally recognised as a fundamental human right. In addition to being addressed in the most important international and regional human rights treaties, some aspect of the right to privacy is incorporated into almost every constitution in the world, and into the general laws and jurisprudence of those countries without written constitutions. [64] Countries that have no written constitutions extend privacy protections through their other legal norms such as procedural rules, evidentiary codes, and statutory protections,[65] so that the protection of

---

[60] *Id.,* para. 11.

[61] *Id.,* paras. 7–9.

[62] See Convention for the Protection of Human Rights and Fundamental Freedoms, 1953, 213 UNTS. 222, Article 8 (European Convention on Human Rights). It states the following:

> (1) Everyone has the right to respect for his privacy and family life, his home and correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

See Article 29 Universal Declaration of Human Rights. The Universal Declaration of Human Rights imposes a general restriction in Article 29 upon the rights recognised in the instrument:

> (1) Everyone has duties to the community in which alone the free and full development of his personality is possible. (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

Article 4 of the International Covenant on Civil and Political Rights specifically states that derogation is possible in time of an emergency. Although Article 4(2) also notes some articles from which derogation is not possible. Since article 17, on the right to privacy, is not mentioned under that provision, it should be assumed that derogation is possible on the right to privacy.

> 1. In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.
> 2. No derogation from articles 6, 7, 8 (paragraphs I and 2), 11, 15, 16 and 18 may be made under this provision.

Articles. 4 and 17 International Covenant on Civil and Political Rights.

[63] *Id.*, Article 32(1); Universal Declaration of Human Rights, Article 29(2).

[64] Edwards, G. E., "International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy", *Yale Journal of International Law*, vol. 26, 2001, 323–412, 327.

[65] One example is the United Kingdom, which lacks a written constitution but has statutory laws and other protections for privacy in place. See Krotoszynski, R. J., "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law", *Duke Law Journal*, vol. 39, ed. 6. 1990, 1398–1454, 1401.

privacy has become a common component of the laws of nearly every country.[66] Given the recognition of the right to privacy in the most important international treaties, the legal acknowledgment of the right to privacy in the majority of legal systems, and the generalised belief among jurists and scholars of the importance of privacy, it can be concluded that this right has become part and parcel of customary international law. Although the right to privacy is not absolute, and must yield when other societal interests are at stake, a balancing test must take into account the universality of the right and the acts it protects,

International law recognises privacy as an important aspect of human dignity. The need to implement adequate protections is exacerbated by the development of new technologies that facilitate the invasion and interference with an individual's privacy.[67] To determine the effect of new technologies on the right to privacy, and provide adequate solutions, a contextual analysis of the potential infringements that technology facilitates and the resources available for protection is essential. Such analysis requires first, an examination of how technological progress has changed individuals' behaviour and affected society as a whole regarding privacy, and then, finding the adequate solutions to address privacy concerns in a manner that embraces the benefits of technological advancement while balancing the individual's right to privacy.

III. The Effect of Information Technologies and the Internet on the Right to Privacy

It is indisputable that the capacity, power, speed, and impact of information technology has been, and continues to be, accelerating rapidly. With these advancements there is also a corresponding increase in the risks to privacy.[68] The demands of a democratic society and its obligations towards protecting individual rights must be balanced against the need and appetite for electronic commerce and information technology. The reality is that technologies that might be invasive of one's privacy also have the potential for unprecedented opportunities for enlightenment, prosperity and security. Traditionally, privacy law has developed in the footsteps of technology constantly reshaping itself to meet the privacy threats embodied in new technologies.[69] The information revolution, however, has been taking place at such speed and affecting so many areas of privacy law that the orthodox, adaptive legislative and judicial process has failed to address digital privacy problems adequately and swiftly. The last generation has seen technological change on a scale matching or exceeding that of the industrial revolution.[70] Three relatively recent major digital developments have affected our concept of privacy greatly. The first of which is the increase in data creation and the resulting collection of vast amounts of personal data—caused by the electronic recording of almost every

---

[66] See Rengel, A. I., *Privacy in the 21st Century*, Martinus Nijhof Publishers, Leiden, 2013, 205–255. The author addresses specific aspects of the right to privacy that have become part of customary international law by looking at treaties, international court decisions, opinions by jurists, commentators and state practice.

[67] Froomkin, A. M., "The Death of Privacy?", *Stanford Law Review*, vol. 52, no. 5, 2000, 1461–1543, 1468.

[68] See Solove, D. J., "Privacy and Power: Computer Databases and Metaphors for Information Privacy", *Stanford Law Review*, vol. 53, ed. 6, 2001, 1393–1462, 1394.

[69] See Hernandez, D. F., "Litigating the Right to Privacy: A Survey of Current Issues", *446 PLI/Pat* 425, 1996, 429.

[70] See Quinn, Jr., E. R., "Tax Implications for Electronic Commerce over the Internet", *Journal of Technology Law and Policy*, vol. 4, ed. 3, 1999.

transaction; secondly, the globalisation of the data market and the ability of anyone to collate and examine this data; and lastly the lack of control mechanisms for digital data which existed to protect analogue data.[71] These three developments all concern the changes wrought by digital technology on the ability to manipulate, store and disseminate information.[72] Every interaction with the Internet and with social networks, every credit card transaction, every bank withdrawal, and every magazine subscription is recorded digitally and linked to specific users.[73] All of this information, once it is collected in networked databases, can be sent instantly and cheaply around the globe.[74] Individuals have little ability to control this collection or manipulation of their data. Most people are not even aware of what information has been collected about them or for what purpose it is being used.[75]

While all of these changes affect information, not only informational privacy has been affected, autonomy is also imperilled from the interference with one's daily life by digital technology and the Internet.[76] When almost every activity leaves a digital trail, government and private monitoring become less about analogue surveillance or human intelligence gathering and more a matter of "data mining," defined as: 'the intelligent search for new knowledge in existing masses of data.'[77] Additionally, when the Internet stores and makes available all types of information previously collected and without any type of filter, individuals' privacy is inevitably affected. The well-documented problem with the current state of privacy law is that it does not factor new advancements in technology or reflect societal and individual notions of privacy.[78]

The explosion in the availability and access to the Internet has made it one of the principal tools for communication, commerce and research. With the hyper development of new technologies and applications, the Internet is constantly evolving for ever more creative uses.[79] However, because of its relative youth in mass application, the Internet lacks many of the protections and control mechanisms utilised for systems like hard-wired telephony. Such things as the unauthorised collection and storage of information

---

71 Berman, J., and Mulligan, D., "Privacy in a Digital Age: Work in Progress" *Nova Law Review*, vol. 23, 1998, 551–582, 553–54.

72 Froomkin, A. M., "The Death of Privacy?", *Stanford Law Review*, vol. 52, no. 5, 2000, 1461–1543, 1462.

73 As compared to old-fashioned cash commerce today's "e-commerce" allows merchants to track your "clickstream" through the use of "cookies," and are able to track your interests based on what you view as well as your purchase, while credit companies are able to record your purchase. See United States Court for the Southern District of New York, *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 501–05, SDNY (2001).

74 Berman and Mulligan, *supra* nt. 71, 554.

75 Solove, "Conceptualizing Privacy", *supra* nt. 31, 1095.

76 See generally Cohen, J. E., "A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace", *Connecticut Law Review*, vol. 28, 1996, 981–1039.

77 See generally Fulda, J. S., "Data Mining and Privacy", *Albany Law Journal of Science and Technology*, vol. 11, 2000, 105–113. In this article, Fulda defines and discusses the concept of data mining. Data mining shows how difficult it is to fully determine the various breaches of privacy because the technology allows the collection and potential for misuse of such vast amounts of data.

78 See Nissenbaum, H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, Palo Alto, 2010, 104–126; Solove, *Understanding Privacy*, *supra* nt. 37, 1–37; Nissenbaum, H., "Privacy as Contextual Integrity", *Washington Law Review*, vol. 79, ed. 1, 2004, 101–139, 119; Nissenbaum, H., "Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy*, vol. 17, ed. 5, 1998, 559–596; Solove, "Conceptualizing Privacy", *supra* nt. 31; Strahilevitz, L. J., "A Social Networks Theory of Privacy", *University of Chicago Law Review*, vol. 72, 2005, 919–988.

79 Pikowsky, R. A., "Legal and Technological Issues Surrounding Privacy of Attorney Client Communications Via Email", *Advocate*, vol. 43, ed. 16, 2000.

relating to Internet activities have emerged as significant threats to privacy on the Internet.[80] With each keystroke and page that is opened, database server's store and catalogue very precise information about the user and his or her use of the Internet. Many sites utilise what are commonly known as "cookies" which are placed on an Internet user's access device and facilitates detailed information about the user often without the user's knowledge or consent. Adding to the amount of personal data collected are the websites that require personal data before use and others that obtain information in connection with purchases, all of which are readily vulnerable to theft and abuse. Sites such as Google, Yahoo, Twitter, Facebook, and LinkedIn, accumulate personal data about users with alarming specificity. They are able to know such things as where individuals log on from, their use patterns and their personal and professional contact information. The collection and retention of this data is a source of great concern but has also been sought by governments and others for non-commercial purposes, such as hackers, businesses and simply the curious.

Social networks have had perhaps the greatest growth as well as the biggest impact on privacy because of the way they have affected how people interact on line. Today, there are some fourteen social media networks with over one hundred million registered users.[81] Most social networks share the common characteristic of 'visible profiles that display an articulated list of Friends who are also users of the system.'[82] As social networks have mushroomed, so has the amount of information and data that individuals are willing and able to post about themselves and others on these sites. Sites such as Facebook, MySpace, Google+, Instagram, etc., collect data on the interests of their users, their friends, and their preferences, for anything from travel information to the games they play. They also collect photographs, location, and many other pieces of information about the users using new technologies such as facial recognition technology. This information becomes the source of much concern from a privacy rights perspective because once the information is uploaded onto a social network, the site has broad latitude as to how long it can maintain the information, how to use the information, and for what purposes.[83]

In addition to identifying information that the users themselves disclose when they sign up for the service, such as their address, telephone number, date of birth, etc., the

---

[80] See Simmons, R., "Technological Change and the Evolution of Criminal Law: Why 2007 is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence", *Journal of Criminal Law and Criminology*, vol. 97, ed. 2, 2007, 531–568, 533. The author discusses the effect of technology on Fourth Amendment cases and argues for an appropriate balance between an individual's right to privacy and the government's interest in law enforcement. See Hornung, M. S., "Note Think Before You Type: A Look at Email Privacy in the Workplace", *Fordham Journal of Corporate and Financial L*aw, vol. 11, 2005, 115–159, 118.

[81] *Facebook* 1+ billion, USA; *Tencent* 712 million, China; *Skype* 663 million, Denmark/Sweden; *Qzone* 536 million, China; *Twitter* 500+ million, USA; *Google*+ 400+ million, USA; *Windows Live* 330+ million, USA; *Sina Weibo* 368 million, China; *Tencent Weibo* 310 million, China; *Habbo* 273 million, Finland; *LinkedIn* 175+ million, USA; *Badoo* 162+ million, UK; *VK (VKontakte)* 140+ million, Russia; *Bebo* 117 million, USA. Wikipedia, *List of virtual communities with more than 100 million users*, available online at <en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_users> (accessed 4 November 2014).

[82] *Ibid.*

[83] Users grant Facebook, for example, 'a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)…' limited only by Facebook privacy settings. Moreover, this "license" does not end upon deletion or closing on one's account. Facebook Statement of Rights and Responsibilities, available online at <facebook.com/legal/terms> (accessed 4 November 2014).

sites also collect information about the device that a user is using to access the site, track data about patterns of use of the service, record location information of the user when they access the site, and may collect other personal information stored in the user's computer using cookies and anonymous identifiers.[84] This ability to capture so much consumer information has not gone unnoticed and in some cases has led to a legal response from governments concerned about the privacy rights of their citizens.

In 2009, Germany passed amendments to the country's Federal Data Protection Act,[85] and has since then battled with United States (US) technology companies Apple, Facebook, and Google. The country launched investigations into how these companies collect and store personal data.[86] In one instance, German officials asked Google to turn over data from home wireless networks that were collected while the company compiled information for its Street View map.[87] German officials also questioned Apple about the duration and the type of personal information the company stores on its iPhone 4.[88] German data-protection officials launched legal proceedings in August 2010 because of how Facebook handles non-user information.[89] Facebook's social graph architecture allows any site to share information between the site and the Facebook platform, permitting readers of the German news magazine Spiegel Online[90] to see what stories their Facebook "friends" like, for example.[91] The Facebook privacy policy, however, suggests that Facebook receives an array of data when a user visits a website that connects to the Facebook Platform through such links as the "Like" button

> We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plug-in). This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.[92]

---

84 *Ibid.*

85 Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Germany, 1 January 2002, BGBl. I, last amended by Gesetz [G], 1 September 2009, BGBl. I.

86 Annual Activity Report 2009/2010 of the Federal Commissioner for Data Protection and Freedom of Information, 23 April 2010, available online at <bfdi.bund.de/SharedDocs/Publikationen/EN/AnnualReport/2009-2010.pdf?__blob=publicationFile> (accessed 1 December 2014). See also New York Times, O'Brien, K., *Despite Privacy Inquiries, Germans Flock to Google, Facebook and Apple*, 11 July 2010, at B8, available online at <http://www.nytimes.com/2010/07/12/technology/12disconnect.html?_r=0> (accessed 1 December 2014).

87 New York Times, O'Brien, K., *Google Balks at Turning Over Data to Regulators*, 27 May 2010, at B3, available online at <nytimes.com/2010/05/28/technology/28google.html> (accessed 4 November 2014).

88 *Ibid.*

89 Wall Street Journal, Lawton, C., and Fuhrmans, V., *Google Rouses Privacy Concerns in Germany—Mapping Service Sparks Debate as Nation Scarred by Authoritarian Past Grapples With Personal Data in Digital Age*,.17 August 2010, at B5.

90 An online magazine available online at <spiegel.de/international/> (accessed 4 November 2014).

91 In 2010, Facebook opened up its powerful platform, allowing any site in the world to connect to Facebook. The Guardian, Bell, E., Why *Facebook's Open Graph Idea Must Be Taken Seriously*, 26 April 2010, available online at <guardian.co.uk/media/pda/2010/apr/26/facebook-f8-emily-bell> (accessed 4 November 2014).

92 Data Use Policy, Facebook, available online at <facebook.com/full_data_use_ policy> (accessed 4 November 2014).

In early 2014, the District Court of Berlin ruled that Facebook has to comply with German data protection law. The Berlin court confirmed a 2012 verdict that found that Facebook's "Friend Finder" violated German law because it was unclear to users that they imported their entire address book into the social network when using it. The court also confirmed that several clauses of Facebook's privacy policy and terms of service violate German law.[93]

France has also seen legal battles involving the likes of social media. In *Hervé G. v. Facebook France*, the Paris Court of First Instance considered a claim brought by French Bishop Hervé Giraud of Soissons against Facebook.[94] Bishop Hervé Giraud of Soissons claimed that a Facebook page titled "Courir nu dans une église en poursuivant l'évêque" (running naked in a church after the bishop) incited hate and violence against Catholics and, thus, violated the French hate speech codes.[95] He also claimed that his photograph was used without his permission.[96] The French court ruled in the bishop's favour on both grounds.[97] Even though the photograph at issue was not at all scandalous, but rather simply a portrait of the bishop,[98] the French court ordered Facebook to remove the page, and to pay 2,000 Euros in damages, with a penalty for every day the page remained up.[99]

In the United States, many courts have attempted to define what the reasonable expectation of privacy in the context of the Internet is, with little success.[100] The case of *Lane v. Facebook*,[101] shows how easy it is for social network sites to have access and share user's information that should remain private. In 2007 Facebook launched the Beacon program where user records were released on the public for friends to see. Mr. Sean Lane bought a diamond ring from overstock.com, and it showed up on his news feed, which was visible to his wife. Along with other plaintiffs, Lane filed a class action suit against Facebook complaining that the Beacon program was causing publication of otherwise private information about their outside web activities to their personal profiles without their knowledge or approval. The parties eventually settled for USD9.5 million in damages, and Facebook ended the Beacon program.

The case of *New York v. Harris* shows the difficulty in determining where the line lies between the private and the public in online communications. The case began in 2011 in the context of the "Occupy Wall Street" movement. After being arrested and charged with disorderly conduct during a particular march across the Brooklyn Bridge, Mr. Harris pled "not guilty" and claimed New York police led protesters on to the Brooklyn Bridge in order to make it easier to arrest them. The Prosecutor subpoenaed Mr. Harris' tweets saying they would reveal that he was "well aware of police instructions" ordering protesters not to block traffic. The New York City District Attorney's Office requested

---

93 District Court of Berlin, *In Re: Facebook*, 5 U 42/1216 0 551/10, 24 January 2014.

94 TGI Paris, 13 April 2010, *Hervé G. v. Facebook France@*.

95 *Ibid.*

96 *Ibid.*

97 *Ibid.*

98 La Vie, Bataille, J., *Condamné pour Outrage à un Évêque, Facebook Gagne en Appel*, 1 November 2011, available online at <lavie.fr/actualite/france/condamne-pour-outrage-a-un-eveque-facebook-gagne-en-appel-11-01-2011-13046_4.php> (providing an image of the Facebook page) (accessed 4 November 2014).

99 *Ibid.*

100 Solove, D. J., "Fourth Amendment Pragmatism", *Boston College Law Review*, vol. 51, 2010, 1511–12. The author explains that '[t]he reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence. Debates rage over whether particular government information activities invade "privacy"'.

101 US Court of Appeals 9th Circuit, *Lane v. Facebook Inc.,* 2012, 696 F.3d 811.

Twitter to turn over reams of information, including the content Harris's of tweets, IP addresses from where he accessed Twitter, and any email addresses it had on file. Harris contested the subpoena alleging that: '[T]he tweets are protected by the Fourth Amendment because the government admits that it cannot publicly access them, thus establishing that the defendant maintains a reasonable expectation of privacy in his communications…' However, the court ruled that Harris did not have legal standing to challenge it because the information—including all of his tweets—belonged to Twitter. The Judge stated

> If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private e-mail, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the Internet that now exist. Those private dialogues would require a warrant based on probable cause in order to access the relevant information.[102]

The Court's decision allowed the government to obtain the content of communication—tweets—with simply a subpoena, and not a search warrant as required by the Fourth Amendment and the Stored Communications Act. Twitter was also ordered to give the keys to location information—IP addresses that could be used to determine where a person is when he logs into Twitter—without a search warrant. On September 13, Twitter turned the requested information over to the judge.

In the case of *Romano v. Steelcase*, another court in the State of New York held that information posted on the Plaintiff's MySpace page was public.[103] Kathleen Romano brought an action against Steelcase Inc. claiming that the defendant permanently injured her so severely that she was confined to misery and home. For the trial the defendant sought to introduce portions of Romano's Facebook and MySpace sites that showed her looking happy, traveling and portraying a lifestyle inconsistent with her litigation claims to the contrary. Defense counsel asked Romano about her Facebook and MySpace data, and sought not only the live private pages but also deleted pages. Romano refused, and the defendant pursued. The court found no reasonable expectation of privacy in social network sites and allowed disclosure information stating that:

When Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. [104]

The United States Supreme Court has been hesitant to issue definitive rulings about Fourth Amendment expectations of privacy pertaining to new technology in an apparent acknowledgement of the difficulty in determining where the public sphere ends the private sphere begins.[105] Cases involving privacy issues and new technologies raise

---

[102] *Ibid*.

[103] New York Supreme Court, 2010, *Romano v. Steelcase, Inc.,* 907 N.Y.S.2d 650.

[104] *Id.,* 657.

[105] See US Supreme Court, 17 June 2010, *City of Ontario v. Quon*, 130 S.Ct. 2619, where the Court found that changes in technology made it difficult to determine reasonable expectations of privacy and declined to issue a ruling about employee privacy expectations when using employer-provided communication devices.

questions about the private/public dichotomy in the context of current laws addressing privacy. Given that Twitter has a feature that allows a user to block a follower, does that feature give the user a sense of control over his messages regarding who has access to them? Are messages posted on Twitter "gifted to the world", or are those messages more like emails, and would require the government to obtain a warrant to have access to them? Is anything published in a MySpace or FaceBook "wall/page" public? What about posts that have been deleted?

In the context of information accessed through a search engine and consequently made available via the Internet through such means, a recent decision from the European Court of Human Rights judicially recognised the "right to be forgotten".[106] This "right" is little more than a long held feeling that an individual should have the ability to remove information from the internet at some point in time based on such reasons as it being incorrect, being unfairly placed on the internet, or simply being having occurred long ago and no longer relevant. The "right to be forgotten" was enshrined in the in the 1995 European Data Protection Directive (Directive 95/46 EC). Under Article 12 of the Directive private citizens in the EU were permitted to request removal of information from the Internet, however, only recently has the Court provided guidelines for the application of such right.

The case began in 2010 when a Spanish citizen presented a complaint against a Spanish newspaper and Google with the Data Protection Agency of Spain. Mr. Costeja alleged that a notice of auction in connection with a bankruptcy notice that appeared in Google's search results violated his right to privacy because the matter to which the notice related had been completely resolved for several years and was no longer relevant. He initially asked the Court to order that the newspaper either delete the information or change the pages at issue so that the personal data would cease to appear online, and also that Google Spain or Google Incorporated not make the information relating to him available through searches with his name.

The Spanish Audiencia Nacional decided to stay the proceedings and to refer the case to the Court of Justice of the European Union. The Grand Chamber found that

> a) Even in cases where the actual server is located outside of the EU, the laws and Directives of the EU are applicable to search engine providers if they maintain a physical presence in any Member State and carry out business intended toward garnering revenue within the EU;
>
> b) Search engines should be considered "controllers" of personal data. That by search engines qualify by "…exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results." As such the right to be forgotten as enshrined in 95/46 EC also applies to them.
>
> c) The Court concluded that the Right to be Forgotten arises not only in cases where the data is inaccurate but also in cases where the information is

[106] European Court of Justice, Grand Chamber, 13 May 2014, *Google Spain v. AEPD and Mario Costeja Gonzalez*, C-131/12.

> inadequate, irrelevant or excessive in relation to the purposes of the processing, in cases that the information is not kept up to date, or in cases where the information is kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.

The European Court also stated that the right to be forgotten is not without limits and must be balanced against 'the legitimate interest of internet users potentially interested in having access to that information…'.[107] Interestingly, the Court made explicit that the party requesting removal need not establish 'that the inclusion of the information in question in the list of results causes prejudice to the data subject.'[108] The issuance of this ruling clarifies that the "right to be forgotten" is more than an aspirational right as may have been previously thought given its existence in the Directive 95/46 since 1995.

Current cases on privacy issues illustrate that in the current technological landscape it is virtually impossible to clearly differentiate the private from the public. The law seems to always be playing catch-up to technology that develops faster than the legal frameworks to regulate it. The impact of digital technology on privacy appears to follow the same pattern seen with older technologies, and one can foresee that the law will attempt to evolve in response to the privacy threats posed by the digital revolution.[109] However, the impact of the digital age is so deep and pervasive that expansion of a single area of privacy law is unlikely to adequately address all of the problems.[110] The response to the effect of new technologies on our concept of privacy has usually been greater governmental regulation.[111] However, greater regulation might not adequately address

---

[107] European Court of Justice, Grand Chamber, 13 May 2014, *Google Spain v. AEPD and Mario Costeja Gonzalez*, C-131/12

[108] *Ibid*.

[109] Cohen, J.E., "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review*, vol. 52, 2000, 1374.

[110] Challis, W.S., and Cavoukian, A., "The Case of a U.S. Privacy Commissioner: a Canadian Commissioner's Perspective", *The John Marshall Journal of Computer and Information Law*, vol. 19, 2000, 1. The author argues that the current regulatory system with regards to new technologies and their effect on privacy is insufficient. He makes the case for the creation of a specialised agency headed by a US Privacy Commissioner with the responsibility of establishing fair information practices and standards in the context of businesses and technologies.

[111] For examples of state regulation initiatives see: Directive 95/46/EC of the European Parliament and the Council of 24 October 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 OJ (L281/33), available online at <europa.eu/legislation_summaries/information_society/l14012_en.htm> (accessed 4 November 2014); Freedom of Information Act, United States of America, 5 USC Section 552 (2000), available online at <usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm> (accessed 4 November 2014); Right to Financial Privacy Act, United States of America, 12 USC Section 3412 (2000), available online at <law.cornell.edu/uscode/text/12/3412> (accessed 4 November 2014); Privacy Protection Act, United States of America, 42 USC Section 2000 (2000), available online at <law.cornell.edu/uscode/42/2000aa.html> (accessed 4 November 2014); Employee Polygraph Protection Act, United States of America, 29 USCS Sections 2001 *et seq.* (2000), available online at <law.cornell.edu/uscode/29/usc_sup_01_29_10_22.html> (accessed 4 November 2014); Cable Communications Policy Act, United States of America, 47 USC Section 551(h) (2000) , available online at <law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000551----000-.html> (accessed 4 November 2014); Financial Services Modernization Act, United States of America, Pub. L. No. 106-102, 113 Stat. 1338 (1999), available online at <gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html> (accessed 4 November 2014); The Children's Online Privacy Protection, United States of America, 15 USC Sections 6501–6506 (1999), available online at <law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_91.html> (accessed 4 November 2014); Personal Information Protection and Electronic Documents Act, Canada, S.C. ch. V (2000) (assented

privacy violations on the part of governments and private parties that utilise the latest technologies. The demands of protecting the right to privacy in Cyberspace must take into account the easiness of access to personal information available online to virtually anyone with a computer, as well as the technological advancements that can facilitate protection. A problem-based approach seems to be the most appropriate approach to arrive at a feasible solution that addresses privacy concerns in Cyberspace. The concept of Obscurity in Cyberspace has been advanced as a way to provide effective and effective remedies to protect the right to privacy in the Internet.[112]

IV. The Right to Obscurity in Cyberspace

The concept of privacy includes the idea that even though human interactions might often take place in public spaces, individuals rely on a zone of privacy that is not open and accessible to others unless the owner agrees to share that space. Given the difficulties in defining an individual's actual zone of privacy, and in trying to design the appropriate safeguards to protect it, especially in the context of Cyberspace, it has been argued that "obscurity" is a more desirable goal.[113] Obscurity is defined as the state of unknowing or being unidentifiable online.[114] An individual is obscure when a casual observer does not possess sufficient information about an individual to decipher the fragments of data about that person that might be accessible in Cyberspace. For example, if two individuals are having a conversation in a restaurant, the casual observer, who has not been previously acquainted with them, and is not eavesdropping, does not possess sufficient information to readily identify the individuals or determine the content of their conversation. In the context of Cyberspace, an individual is obscure when critical information such as identity, social connections, and other personal information is not readily available or decipherable by others.[115] Online obscurity has been defined as information that 'exists in a context missing one or more key factors that are essential to discovery or comprehension.'[116]

The intrinsic need to keep certain areas of our lives private is evident when one looks at the actual content of the Internet. It has been estimated that 80-99 percent of the World Wide Web is completely hidden from general-purpose search engines and only accessible by those with the right search terms, URL, or insider knowledge.[117] Other

---

to Apr. 13, 2000), available online at <priv.gc.ca/information/guide_e.pdf> (accessed 4 November 2014); The Australian Privacy Commission, Australia's Privacy Amendment (Bill 2000), Australia, available online at <privacy.gov.au/law/act> (accessed 4 November 2014).

112 Hartzog. W., and Stutzman, F., "The Case for Online Obscurity", *California Law Review*, vol. 101, 2013, 1–52.

113 Hartzog, W. and Stutzman, F., "Obscurity by Design", *Washington Law Review,* vol. 88, ed. 2, 2013, 385. The authors juxtapose "privacy by design" as a universal approach to privacy which poses a set of significant challenges for implementers with "obscurity by design" as the optimal protection for most online social interactions. The authors propose that information in cyberspace can be plotted on a spectrum of obscurity that would allow regulators, designers, and organisational stakeholders to adopt guiding principles regarding the protection of online information.

114 Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112, 5.

115 *Ibid.*

116 *Id.*, 35.

117 'Since they are missing the deep Web when they use such search engines, Internet searchers are therefore searching only 0.03%—orone in 3,000—of the pages available to them today', Bergman, M. K., "The Deep Web: Surfacing Hidden Value", *The Journal of Electronic Publishing*, vol. 7, ed. 1, 2001, available online at <quod.lib.umich.edu/cgi/t/text/textidx?c=jep;view=text;rgn=main;idno=3336451.0007.104>

pieces of online information are obfuscated by the use of pseudonyms, multiple profiles, privacy settings, or encryption.[118] The constant effort made by many to keep certain information obscure from the casual Internet user shows the need for humans to maintain a sphere of privacy. On the Internet, information that is obscure has very little chance of being understood by unintended recipients. Consequently, although a user might choose to make some information public, they also want the prerogative to limit the recipients of certain information that he/she might wish to remain private. Such user control provides adequate protection from online privacy infringement.

Obscurity can be achieved by the creation of design-based solutions for new technologies that would benefit from increased attention to user interaction, with a focus on the principles of "obscurity" rather than the expansive and vague concept of "privacy".[119] Obscurity in cyberspace, in part, is achieved by requiring the protection of access to identifying information related to users. Access protection covers a variety of technology and methods to manage access to content.[120] Obscurity can also be achieved through regulation that protects an individual's information mandating that information that a user wishes to remain private be kept secure and unidentifiable. To the extent that a fundamental right to privacy has been internationally recognised, and given that the Internet has become an extension of our social sphere, it can be argued that a right to "obscurity" in Cyberspace is an indispensable corollary to the right to privacy. Hartzog and Stutzman have made a good case for Online Obscurity and Obscurity by Design as alternatives to creating other frameworks for privacy protection on the Internet.[121] They have convincingly argued that the "right to obscurity" in Cyberspace should be easier to implement than the difficult to define right to privacy and the behaviours that might constitute breach of the right to privacy in Cyberspace. Obscurity could serve as a compromise protective remedy: instead of forcing websites to remove sensitive information, courts could mandate some form of obscurity.[122] Internet "companies" bound by a "duty to maintain obscurity" would be allowed to further disclose information online, so long as they kept the information generally as obscure as the form in which they received it.[123] Finally, obscurity could replace confidentiality as a term in some contracts, particularly those involving the Internet.

Similarly, the right to obscurity in Cyberspace, requiring certain providers to allow for users to keep their information obscure, and allowing greater certainty for courts and administrative bodies in determining what information should be considered private

---

(accessed 27 October 2014); Medeiros, N., "Reap What You Sow: Harvesting the Deep Web", *OCLC Systems and Services*, vol. 18, ed. 1, 2002, 18–20.

[118] 'Most people believe that security through obscurity will serve as a functional barrier online. For the most part, this is a reasonable assumption.', Boyd, D., "Why Youth Heart Social Network Sites: The Role of Networked Publics in Teenage Social Life", *in:* Buckingham, D., ed., *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*, MIT Press, Cambridge, 2007, 16; 'People also have a sense that their social-network information will be kept private because they feel anonymous amidst the millions of social-network users.', Keats Citron, D., "Fulfilling Government 2.0's Promise with Robust Privacy Protections", *George Washington Law Review,* vol. 78, ed. 4, 2010, 835; Gelman, L. A., "Privacy, Free Speech, and "Blurry-Edged" Social Networks", *Boston College Law Review*, vol. 50, ed. 5, 2009, 1317–18; Grimmelmann, J., "Saving Facebook", *Iowa Law Review,* vol. 94, ed. 4, 2009, 1160–63.

[119] Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112.

[120] *Id.*, 37–38.

[121] Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112; Hartzog and Stutzman, "Obscurity by Design", *supra* nt. 113.

[122] Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112, 3.

[123] *Ibid*.

would be beneficial for all. There are four factors which when found diminish obscurity (and their absence enhances it) and that could be used by judges and others to determine whether certain information on the Internet is private or public, these are: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity.[124] Having clear guidelines as to what constitutes private versus public information from a legal standpoint would benefit users by providing some degree of clarity and expectation regarding what information about them is considered to be legally private. Likewise, courts would have a uniform framework to establish privacy protections in Cyberspace. When a judge is faced with a situation where the sphere of privacy must be determined, looking at the above factors can facilitate a determination on whether the information should be considered to be public or private. These factors can also be applied uniformly to provide standard guidelines that may be universally adopted to protect privacy online.

The right to obscurity should also place the burden on service providers and technology manufacturers to create technology that provides users with the possibility to maintain the obscurity of certain information if they choose to do so. These guidelines should take into account the available tools for users to indicate their intentions regarding the information that they want to keep private. The four factors should become guidelines for the manufacturing of appropriate technology as well as the necessary regulation to achieve such ends.

Whether the right to obscurity is an extension of the right to privacy is an argument based on the importance that individuals place on privacy, the acknowledged legal recognition of a right to privacy in the international context, the need to adapt our concept of privacy to new technologies, and the lack of current legal guidelines that provide appropriate safeguards to protect users from privacy infringements on the internet. The right to privacy as an abstract concept is insufficient to protect individuals' privacy given the technology available to infringe it. However, if the right to privacy is an internationally recognised right, the right to obscurity might serve to give substance to the right for individuals who are concerned about the effect of current communications on their privacy. Additionally, using the four factors to determine whether certain information was meant to remain obscure online, courts should be able to identify a clear line that divides the private from the public eliminating the current confusion regarding the right to privacy online.

V. Conclusion

The concept of privacy has been discussed for centuries by philosophers, anthropologists, sociologists, and legal scholars. The importance that individuals place on privacy is beyond question and transcends geographical, cultural and racial boundaries. Individuals' need for secrecy and private space is so fundamental to forging relationships with others and to preserving our sense of self, that a society with a complete lack of individual privacy would be unimaginable. Given that a desire for privacy is a fundamental human characteristic, the idea of a right to privacy follows from our ingrained need for a life of dignity.

At the international level there is evidence of an existing appreciation for the existence of some universal basic principles that merit international legal protection. The concept of a human right can be described as a claim of a higher order than other legal

[124] Hartzog and Stutzman, "Obscurity by Design", *supra* nt. 113, 397.

relationships, such as contractual rights or statutory entitlements.[125] Today, the right to privacy has been recognised as a '…[f]undamental human right that has been defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others and free from State intervention and free from excessive unsolicited intervention by other uninvited individuals.'[126] The argument that the right to privacy has risen to the level of international law can be made and is bolstered by the inclusion of the right in numerous international and regional human rights treaties and its recognition as customary international law. Although the right to privacy is not an absolute right, and must be balanced against state interests, the notion of necessity implies that the interference corresponds to a pressing social need and that it is proportionate to the legitimate aim pursued.[127]

The importance that the right to privacy has for individuals is evidenced in the manner in which the right continues to expand and evolves to adapt to society's needs. The legal definition as well as the contours of what the individual right to privacy encompasses is still and will continue developing as society advances and as technology provides new ways in which individual privacy is affected. The advent of new technologies capable of easily infringing our private affairs has forced us to recognise the pressing need to establish with clarity what level of protection we can expect from governments with respect to our right to privacy. The technologies and ease of communication in today's world have helped individuals recognise that the concept of privacy is more than an abstract notion, and that we must actively seek its protection in order to enjoy the type of freedom that society strives to reach.

Technology brings about innovation and progress for civilisation, but it also brings the potential to harm society and the principles we cherish as individuals. Privacy becomes more of a concern in response to events and advancements that facilitate its infringement. As technology has made the collection, distribution, and transfer of information faster and more efficient, the legal protections available for private personal data have become a necessity. The main problem with establishing a workable framework to determine what is private versus public information on the Internet is that the new communication systems and technologies breach the barrier of what used to be recognisable as private. As technology advances it becomes easier to access individuals' personal information without much effort or training, merely by pressing a button on a computer terminal. Today that data protection appears to be at the forefront of privacy concerns, people are worried about losing their privacy and governments are responding to people's demand for privacy by enacting laws that protect privacy in this digital era. However, the current legal framework of privacy protection in the context of online technologies is unclear and insufficient to deal with the current technology in this area, with its potential to infringe on privacy rights. Fortunately, while there is technology available capable of infringing on online privacy, there is also technology available to help users to keep their digital

---

[125] Dworkin, R., *Taking Rights Seriously,* Harvard University Press, Cambridge, 1977.

[126] United Nations Human Rights Council, Scheinin, M., *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 28 December 2009, available online at <ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> (accessed 27 October 2014).

[127] In *Olson v. Sweden*, the Court stated that, 'the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued; in determining whether an interference is "necessary in a democratic society", the Court will take into account that a margin of appreciation is left to the Contracting States'. European Court of Human Rights, *Olson v. Sweden,* 24 March 1988, 11 EHRR 259, para. 67.

information private.[128] Perhaps the answer is to require that online users be allowed to decide what information they desire to keep public and what information they want to make public.

The concept of obscurity provides a potential bedrock for protecting privacy in Cyberspace. The proposition that there might be a developing right to obscurity in Cyberspace is related to the fundamental need "to be left alone" even in the context of online communications. As a legal concept it may go hand in hand with the recognition of the sanctity of an individual's right to privacy. In the quest for real and verifiable measures that guarantee a level of protection to safeguard privacy in the digital age, obscurity may be an indispensable part of reaching that goal. While the concept of privacy might be difficult to define, the concept of obscurity and the four factors that determine whether information is obscure, might facilitate the creation of standard legal guidelines to make the distinction between public and private and thereby offer real protection for privacy rights in the context of online communications. Society must find a way to adapt to new developments in order to preserve its values and its humanity. It is difficult to predict, or even to imagine future technologies, but positive strides are being made in the recognition that the protection of privacy is everyone's concern and everyone should be involved in protecting the human values it represents.

*

www.grojil.org

[128] See, e.g., PrivacyFix, which is a programme that helps set up a user's privacy settings on Facebook and Google, and control cookie activity. PrivacyFix is available online at <privacyfix.com/start> (accessed 27 October 2014); See (reviewing and explaining the benefits of Privacy), Fix: Cnet, Whitney, L., *Privacy Fix helps protect your privacy on the Web,* 10 October 2012, available online at <news.cnet.com/8301-1009_3-57529655-83/privacyfix-helps-protect-your-privacy-on-the-web/> (accessed 27 October 2014).

The European Union and the Search for an International Data Protection Framework

Christopher Kuner*

Keywords
PRIVACY; DATA PROTECTION; EUROPEAN UNION; INTERNATIONAL LAW; INTERNET

Abstract
The European Union (EU) has supported the growing calls for the creation of an international legal framework to safeguard data protection rights. At the same time, it has worked to spread its data protection law to other regions, and recent judgments of the Court of Justice of the European Union (CJEU) have reaffirmed the autonomous nature of EU law and the primacy of EU fundamental rights law. The tension between initiatives to create a global data protection framework and the assertion of EU data protection law raises questions about how the EU can best promote data protection on a global level, and about the EU's responsibilities to third countries that have adopted its system of data protection.

I. Introduction

In 2009, the author considered the opportunities and difficulties of creating an international legal framework for data protection and privacy.[1] Since then, the globalization of data processing and the Snowden revelations that came to light in the summer of 2013[2] have led to an increased interest in regulating data protection at the international level. It is thus time to revisit some of the points discussed earlier, focusing in particular on EU law as the most influential body of data protection law worldwide.

The trans-border nature of data processing on the Internet has led to increased interest in the possibility of regulating data protection on an international level. Individuals, whose data are routinely transferred around the world via the Internet, often do not know to whom to turn to protect their rights. Companies are frustrated by the lack of harmonisation and the fact that they are often subject to conflicts between data protection law and other legal obligations.[3] And data protection authorities (DPAs), many of whom

---

* Director, Brussels Privacy Hub, Vrije Universiteit Brussel (VUB); Associate Professor of Law, University of Copenhagen; Senior Privacy Counsel, Wilson Sonsini Goodrich & Rosati, Brussels; Honorary Fellow, Centre for European Legal Studies, University of Cambridge. This article is written in the author's personal capacity, and is current as of July 2014. The author is grateful to Hielke Hijmans for his valuable comments on an earlier draft.

1 Kuner, C., "An international legal framework for data protection: issues and prospects", *Computer Law & Security Review*, vol. 25, 2009, 307–317. Strictly speaking, data protection law, which restricts the processing of data relating to an identified or identifiable person, and grants persons rights in the processing of data relating to them, is closely related to, but distinct from, the concept of "privacy". See Kokott, J. and Sobotta, C., "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, vol. 3, ed. 4, 2013, 222–228. However, the two terms will be used synonymously here for the sake of convenience, unless otherwise noted.

2 See regarding the Snowden revelations Greenwald, G., *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, MacMillan, New York, 2014.

3 For example, with regard to conflicts between data protection law and civil litigation rules in the US. See, e.g., Article 29 Working Party, "Working Document 1/2009 on pre-trial discovery for cross border civil litigation" (WP 158, 11 February 2009).

lack sufficient resources to carry out their tasks, often have to deal with complex questions involving data processing that takes place in other regions.

Existing instruments dealing with the international regulation of data protection all have various shortcomings. International human rights instruments protect the processing of personal data,[4] but they are typically not detailed enough to provide individuals with a direct remedy in individual cases. In 1990 the UN adopted guidelines concerning computerised personal data files, which have had little practical impact.[5] The UN General Assembly passed a resolution on 18 December 2013 that affirms the online application of the right to privacy,[6] and the UN Human Rights Commission is working to promote the right to privacy in the digital age,[7] but these initiatives are by themselves unlikely to lead to a complete solution.

There have been growing calls for a stronger international legal framework for data protection. For example, in 2005 the 27th International Conference of Data Protection and Privacy Commissioners issued the "Montreux Declaration", in which it appealed to the United Nations 'to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'.[8] Since then, further instances of the International Conference have adopted similar resolutions.[9] Some companies have also made such appeals; for example, in 2007, Google called for the creation of "global privacy standards".[10] Civil society groups have also called for global standards.[11]

EU institutions and Member States have been particularly active in promoting global data protection standards. Thus, the Article 29 Working Party (the group of DPAs from the EU Member States) has stated that 'global standards regarding data protection are becoming indispensable',[12] and that it supports 'the development of a global instrument

---

4 Universal Declaration of Human Rights (UDHR), 1948, Article 12; ICCPR International Covenant of Civil and Political Rights (ICCPR), 1966, Article 17. See GA Resolution 68/167 (68th session) A/RES/68/167, 18 December 2013.

5 UN Guidelines concerning Computerized Personal Data Files, E/CN.4/1990/72, 14 December 1990. See Bygrave, L., *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014, 2272 (Kindle edition), stating that the UN Guidelines "have had a lower public profile and practical impact than the majority of the other main international instruments...".

6 GA Resolution 68/167 (68th session) A/RES/68/167, 18 December 2013.

7 United Nations, Office of the High Commissioner of Human Rights, *The Right to Privacy in the Digital Age*, at <ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx> (accessed 30 June 2014).

8 Privacy Conference, 27th International Conference of Data Protection and Privacy Commissioners, *The Protection of Personal Data and Privacy in a Globalised World: a Universal Right respecting Diversities*, 14–16 September 2005, available online at <privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf> (accessed 20 June 2014).

9 See, e.g., Privacy Conference, 35th International Conference of Data Protection and Privacy Commissioners, *Resolution on Anchoring Data Protection and the Protection of Privacy in International Law*, 23–26 September 2013, available online at <privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf> (accessed 20 June 2014).

10 Google Public Policy Blog, Peter Fleischer, *Call for Global Privacy Standards,* available online at <googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html> (accessed 20 June 2014).

11 The Public Voice, *The Madrid Privacy Declaration, Global Privacy Standards for a Global World*, 3 November 2009, available online at <thepublicvoice.org/madrid-declaration/> (accessed 20 June 2014).

12 Article 29 Working Party, "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data" (WP 168, 1 December 2009), 10.

providing for enforceable, high level privacy and data protection principles.'[13] In 2009 a group under the leadership of the Spanish DPA published "The Madrid Resolution", which is a set of international standards for data protection and privacy.[14] And a number of EU Member States (Austria, France, Germany, Ireland, Luxembourg, Slovenia, and Spain) were among those proposing the UN General Assembly resolution that was passed in December 2013.[15]

At the same time, EU institutions have worked to promote the adoption of EU data protection law as a global standard. For example, the Vice-President of the European Commission Viviane Reding has stated that 'Europe must act decisively to establish a robust data protection framework that can be the gold standard for the world'.[16] And an unnamed EU official has been quoted as saying 'with these proposals, the EU is becoming the de facto world regulator on data protection'.[17]

The principle that the EU legal system constitutes an independent, autonomous source of law has been recognized since the 1960s.[18] The Court of Justice of the European Union (CJEU) has recently proclaimed its autonomous nature and the primacy of EU fundamental rights law in the context of the Treaty of Lisbon, which entered into force on 1 December 2009.[19] As will be discussed below, the Court's recent judgments have also reaffirmed the application of European data protection law to data processing carried out in other regions.

Thus, while EU institutions have called for the development of international data protection standards, they have also emphasized the autonomous nature of EU law and have sought to advance the adoption of EU data protection law around the globe. The EU's involvement in both these phenomena illustrates the tensions inherent in simultaneous developing global values and asserting regional ones, and raises the question of how the EU can best advance the spread of data protection rights around the world. These activities also illustrate how the EU's global influence should be coupled with a global responsibility towards other States that adopt its standards.

---

[13] Article 29 Working Party, "Opinion 04/2014 on surveillance for electronic communications for intelligence and national security purposes" (WP 215, 10 April 2014), 3.

[14] Privacy Conference, International Conference of Data Protection and Privacy Commissioners, *The Madrid Resolution, International Standards on the Protection of Personal Data and Privacy*, 5 November 2009, available online at <privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf> (accessed 22 September 2014).

[15] GA Resolution 68/167 (68th session) A/RES/68/167, 18 December 2013.

[16] Viviane Reding, "A data protection compact for Europe", 28 January 2014, available online at <europa.eu/rapid/press-release_SPEECH-14-62_en.htm> (accessed 22 June 2014).

[17] European Voice, Vogel, T., *Reding seeks overhaul of data protection rules*, 15 December 2011, available online at <europeanvoice.com/article/reding-seeks-overhaul-of-data-protection-rules/> (accessed 4 July 2014).

[18] E.g. European Court of Justice, 5 February 1963, *Van Gend en Loos,* C-16/62, ECR 1963 p. 1; European Court of Justice, 15 July 1964, *Costa v ENEL*, C- 6/64 , ECR 1964 p. 585 . See also van Rossem, J. W., "The Autonomy of EU Law: More is Less?", *in*: Wessel, R. A. and Blockmans, S., *The EU Legal Order under the Influence of International Organisations*, TMC Asser Press, The Hague, 2013, 13.

[19] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 17 December 2007, 2007/C 306/01.

II. Prospects for an international legal framework

II.1. Varieties of international initiatives

The variety of data protection guidelines, conventions, and other instruments that have been enacted at an international level complicate the prospects of reaching agreement on a single international framework. The differences between them can be can be classified in various ways, such as the following:

Legally binding/non binding: Some of these instruments have binding legal effect. Thus, the EU Data Protection Directive 95/46[20] obligates the EU Member States to implement its provisions (i.e. to reflect them in their national law), and individuals may rely on the Directive to assert their rights.[21] The Council of Europe Convention 108[22] legally obligates States that are parties to it to enact its protections into their domestic law, but cannot be relied on by individuals to create legal rights.[23] The OECD Privacy Guidelines,[24] the APEC Privacy Framework,[25] the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection,[26] and the UN General Assembly Resolution of 18 December 2013 affirming application of the right to privacy to online activities[27] are not legally binding.

International/regional: Some initiatives have been enacted at the regional level and others at the international level. International human rights treaties and instruments adopted by UN bodies are obviously applicable on a global scale. The APEC Privacy Framework is applicable to the twenty-one member countries of the Asia-Pacific Economic Cooperation group, and is thus an example of a regional instrument. The Council of Europe Convention 108 is difficult to categorize, since it was initially enacted

---

[20] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available online at <europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm> (accessed 22 September 2014).

[21] See, e.g., European Court of Justice, 24 November 2011, *ASNEF and FECEMD v. Administración del Estado*, Joined Cases C-468/10 and C-469/10 [2011] ECR I-0000; European Court of Justice, 20 May 2003, *Rechnungshof*, Joined Cases C-465/00 and C-138/01 [2003] ECR I-4989.

[22] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, available online at <conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (accessed 22 September 2014).

[23] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, Explanatory Report, para. 38.

[24] The Organisation for Economic Co-operation and Development, *OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, 11 July 2013, available online at <oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> (accessed 22 September 2014).

[25] Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2005, available online at <apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx> (accessed 20 June 2014).

[26] The Economic Community of West African States, *Supplementary Act on Personal Data Protection*, 16 February 2010, available online at <statewatch.org/news/2013/mar/ecowas-dp-act.pdf> (accessed 20 June 2010).

[27] GA Resolution, *supra* nt. 15. See regarding the background of the Resolution Social Science Research Network, Milanović, M., *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 31 March 2014, available online at <papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485> (accessed 29 June 2014).

on a regional (i.e. European) scale and is closely entwined with EU law,[28] but is now open for enactment by States in other regions.[29]

Institutional/ad hoc: Some initiatives that have been established within the framework of an existing institution, while others were drafted on an ad hoc basis. For example, the Council of Europe Convention 108 is administered and promulgated by the Council of Europe, and is interpreted by the European Court of Human Rights. An example of an ad hoc initiative is the Madrid Resolution, which is a declaration drafted under the leadership of the Spanish DPA with the participation of other DPAs, private sector entities, NGOs, and other organizations from around the world.

II.2. Continuing challenges

The challenges for realizing a stronger legal framework at the international level remain much as described in 2009.[30] Despite the growing international recognition of data protection and interest in the possibility of having the Council of Europe Convention 108 serve as the basis for an international data protection standard,[31] considerable differences still exist in the approaches to data protection around the world,[32] owing to cultural, historical, and legal factors, and there is a lack of consensus as it can best be strengthened on an international scale. Thus, there is no agreement as to whether the global framework for data protection should be legally binding or not; whether existing instruments can be used, or a new one is needed; what the substance of any data protection standards should be, and their scope; and what institution should coordinate the work. Indeed, in many cases it is not even clear what the calls by different stakeholders for "global standards" or an "international framework" for data protection mean in concrete terms.

This means that reaching agreement on the substance of an international framework will not be easy. There are two issues of particular importance. First of all, it would be necessary to agree on the level at which such standards should be enacted: if they are too abstract, they may not be able to protect personal data in practice, while any standards that are too detailed may be difficult to implement locally, given the differences in legal cultures around the world. Thus far, most international initiatives concerning data

---

[28] See Consolidated version of the Treaty on European Union (TEU), 9 May 2008, 2008/C 115/01, Article 6, indicating that the European Convention on Human Rights (on which the Convention 108 is based) is recognized by EU law and *de facto* incorporated into it.

[29] So far one non-member of the Council of Europe, namely Uruguay, has enacted the Convention. See Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Treaty open for signature by the member States and for accession by non-member States*, available online at <conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG> (accessed 30 June 2014). The Convention is also in force in non-EU States such as Azerbaijan, Georgia, Russia, and the Ukraine.

[30] See Kuner, *supra* nt. 1, 315–317.

[31] See, e.g., Council of Europe, Polakiewicz, J., *Convention 108 as a Global Privacy Standard?*, 17 June 2011, available online at <coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Convention_108as_a_global_privacy_standards_June_2011.pdf> (accessed 30 June 2014); Social Science Research Network, Greenleaf, G., '*Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?*, 8 May 2013, available online at <papers.ssrn.com/sol3/papers.cfm?abstract_id=2262296> (accessed 30 June 2014).

[32] See Bygrave, *supra* nt. 5, location 6168 (Kindle edition).

protection set the agenda and formulate broad principles, but do not specify how they are to be implemented in detail.[33]

Second, there is no consensus as to which international organization could coordinate the work. Indeed, in the author's experience most international organisations are wary of beginning work on a legally binding data protection instrument because of the political difficulties of reaching agreement, and would hesitate to do so failing a clear mandate from their members. While the UN has the necessary global membership, the work of legal harmonisation bodies such as the United Nations Commission on International Trade Law (UNCITRAL) demonstrates that in the highly politicised atmosphere of the UN, harmonisation even of technical topics tends to proceed slowly and with difficulty.[34] The UN also lacks detailed expertise in the field of data protection.

Thus, the possibility of a global, legally binding data protection instrument being enacted in the foreseeable future remains elusive.

III. EU data protection law in a global context

III.1. Legislative and regulatory activity

EU data protection law has been influential in a global context in two ways: first, by serving as a model for the enactment of data protection law in other regions, and second, by its extraterritorial application to data processing in third countries.

The EU Data Protection Directive has had a substantial influence on the enactment of data protection law in other States,[35] and in particular has influenced States without their own tradition of data protection to enact laws based on the EU model.[36] EU external action policy seeks to promote adoption of EU data protection law in third countries as an aspect of furthering the rule of law, including financing technical assistance projects that allow data protection experts from the EU to work with third countries.[37] More developed States have also been influenced to enact new data protection laws, or update their existing ones, based on EU law.[38] It seems that the EU expects its proposed General Data Protection Regulation[39] to have similar influence.[40]

---

[33] De Hert, P. and Papakonstantinou, V., "Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?", *I/S: A Journal of Law and Policy for the Information Society*, vol. 9, ed. 2, 2013, 271–324, 275.

[34] Based on the author's experience as a longstanding member of the UNCITRAL Working Group on Electronic Commerce and participation in its work on topics such as electronic signatures.

[35] De Hert and Papakonstantinou, *supra* nt. 33, 287–288.

[36] See, e.g., Bygrave, *supra* nt. 5, location 6125 (Kindle edition), stating 'the overwhelming bulk of countries that have enacted data privacy laws have followed, to a considerable degree, the EU model…'; Greenleaf, G., "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108", *International Data Privacy Law*, vol. 2, no. 2, 2012, 68–92.

[37] See Pech, L., "Rule of law as a guiding principle of the European Union's external action", Centre for the Law of EU External Relations (CLEER), T.M.C. Asser Instituut, available online at <asser.nl/upload/documents/2102012_33322cleer2012-3web.pdf> (accessed 4 July 2014), 17–20. For an example of such assistance given in 2011 by the EU focused on 'ensuring the data protection accreditation of Mauritius with the European Union', see <eeas.europa.eu/delegations/mauritius/eu_mauritius/development_cooperation/technical_cooperation/index_en.htm> (accessed 4 July 2014).

[38] See, e.g., New Zealand Privacy Commissioner, "Privacy amendment important for trade and consumer protection", 26 August 2010, available online at <privacy.org.nz/news-and-publications/statements-media-releases/updated-media-release-30-8-10-privacy-amendment-important-for-trade-and-consumer-

EU data protection law can apply extraterritorially to personal data processed in other regions,[41] which expands its influence beyond the geographic borders of the EU. For example, standard contractual clauses for data transfer approved by the European Commission obligate data importers outside the EU to agree to audits at the request of data exporters and, 'where applicable, in agreement with the Supervisory Authority' (for example, the DPA of the EU Member State with jurisdiction over the transfer), as well to submit itself to the authority of the DPA and the EU court with jurisdiction over it.[42]

The applicable law regime of the proposed Regulation would be even more expansive than at present. Under the EU Data Protection Directive, EU law applies extraterritorially primarily in situations when a non-EU data controller uses 'equipment' situated in the EU to process personal data,[43] whereas under the Regulation it would apply in cases where non-EU controllers offer goods or services to individuals in the EU or monitor their behaviour.[44] By doing away with the requirement that equipment situated in the EU be used in order for EU law to apply, the new applicable law regime of the Regulation 'seems likely to bring all providers of Internet services such as websites, social networking services and app providers under the scope of the EU Regulation as soon as they interact with data subjects residing in the European Union'.[45]

Since 2009, the EU legal framework for data protection has also been reinforced by the Treaty of Lisbon. The Lisbon framework creates stronger protection for data protection as a fundamental right, by including a new provision in the Treaty on the Functioning of the European Union (TFEU) that explicitly grants individuals a right to data protection,[46] and by granting full legal effect to the Charter of Fundamental Rights of the European Union.[47]

---

protection/> (accessed 4 July 2014), regarding the influence of EU law on the reform of the New Zealand Privacy Act.

39 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012.

40 See the speech by European Commission Vice-President Viviane Reding, *supra* nt. 16.

41 See, e.g., Kuner, C., "Data protection law and international jurisdiction on the Internet (Part 2)", *International Journal of Law and Information Technology*, vol. 18, no. 3, 2010, 227–247, 228–234; Svantesson, D. J. B., *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, Copenhagen, 2013, 89–111.

42 See Commission Decision (EC) 2001/497 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive (EC) 95/46 [2001] OJ L181/19, Clauses 5(d) and 7(1); Commission Decision (EC) 2001/16 of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46 [2002] OJ L6/52, Clauses 5(f) and 7(1).

43 Directive, Article 4(1)(c).

44 General Data Protection Regulation, *supra* nt. 39, Article 3(2).

45 Svantesson, *supra* nt. 41, 107. See Article 3(2) of the Proposed Regulation.

46 Consolidated version of the Treaty on the Functioning of the European Union (TFEU), [2010] OJ C83/47, Article 16(1). See regarding the strengthened position of data protection as a fundamental right under the Lisbon framework Hijmans, H. and Scirocco, A., "Shortcomings in EU data protection in the third and second pillars. Can the Lisbon Treaty be expected to help?", *Common Market Law Review*, vol. 46, 2009, 1485–1525.

47 Consolidated version of the Treaty on European Union (TEU), *supra* nt. 28, Article 6. See Charter of Fundamental Rights of the European Union, [2010] OJ C83/2, Article 8, which also grants a right to data protection.

III.2. CJEU judgments

The CJEU's first case dealing with the global application of EU data protection law was the *Lindqvist* judgment of 2003,[48] in which the Court found that there is no data transfer to a third country within the meaning of Article 25 of the EU Data Protection Directive when an individual in a Member State loads personal data onto an Internet page which is stored on a site hosted within the EU. The Court's decision was based in part on the fact that finding that a data transfer occurred in this case would effectively make the entire Internet subject to EU data protection law.[49] In this early judgment, the CJEU thus took into account the impact of extending the territorial scope of EU data protection law to the global Internet.

A judgment from outside the field of data protection is of crucial importance for understanding the legal status given to fundamental rights in the EU legal system. In its first *Kadi* judgment,[50] which was issued on 3 September 2008 just before the Lisbon framework came into effect, the CJEU annulled the EU implementation of a UN Security Council resolution that had resulted in the claimant's assets being frozen, finding that it violated his fundamental rights.[51] In particular, the Court noted that even if obligations imposed by the UN Charter were classified as part of the hierarchy of EU legal norms, they would still rank lower than general principles of EU law, including fundamental rights.[52] The Court also re-affirmed the autonomy of the EU legal order,[53] and found that EU implementation of a Security Council resolution is a matter for the 'internal and autonomous legal order of the Community'.[54] The *Kadi* judgment thus affirmed both the position of fundamental rights in the EU legal order, and its autonomous and inward-looking nature.[55]

The influence of the Lisbon framework was demonstrated in the Court's decision in *Digital Rights Ireland*[56] from April 2014, in which it invalidated the EU Data Retention Directive.[57] The decision was based on fundamental rights law and the application of data protection law outside the EU was not directly at issue. However, the Court stated as follows towards the end of the judgment (paragraph 68)

---

48 Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

49 *Id.*, para. 69.

50 Joined Cases C-402 & 415/05P, *Kadi & Al Barakaat Int'l Found. v. Council & Commission*, [2008] ECR 1-6351. The case has resulted in further litigation; see Joined Cases C-584/10 P, C-593/10 P and C-595/10 P Kadi, 18 July 2013. There have also been other cases involving challenges to the implementation of UN sanctions brought under fundamental rights law before both the CJEU and the European Court of Human Rights. See de Búrca, G., "The European Court of Justice and the International Legal Order after Kadi", *Harvard International Law Journal*, vol. 51, 2010, 1-49; Ziegler, K., "Strengthening the Rule of Law, but Fragmenting International Law: the *Kadi* Decision of the ECJ from the Perspective of Human Rights", *Human Rights Law Review*, vol. 9, 2009, 288–305.

51 *Kadi*, para. 351.

52 *Id.*, paras. 305–309.

53 *Id.*, para. 316.

54 *Id.*, para. 317.

55 See regarding the inward-looking nature of the Court's judgment de Búrca, *supra* nt. 50, 41, stating 'the judicial strategy adopted by the ECJ in *Kadi* was an inward-looking one which eschewed engagement in the kind of international dialogue that has generally been presented as one of the EU's strengths as a global actor'.

56 C-293/12 and C-594/12, 8 April 2014.

57 Directive (EC) 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive (EC) 2002/58, [2006] OJ L105/54.

> [I]t should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data…[58]

The criticism in this passage of the Data Retention Directive for failing to require that data be stored in the EU, and the statement that storage outside the EU removes the possibility of supervision by an EU DPA, seems to logically imply that oversight of data processing by the DPAs may also be required with regard to EU data that are transferred to other regions. This conclusion raises a number of questions that the Court did not explore further (e.g., how such extraterritorial supervision could be reconciled with the fact that the enforcement jurisdiction of the DPAs ends at the borders of their respective EU Member States[59]).

The extraterritorial application of EU data protection law was re-affirmed more strongly in *Google Spain v. AEPD and Mario Costeja Gonzalez*[60] from May 2014. One of the issues in this case was whether EU data protection law could apply when a company (in this case Google) has an establishment in an EU Member State that promotes a search engine that orients its activity towards the inhabitants of that State, even though the actual data processing is carried out by the establishment's parent company located outside the EU. In finding that EU data protection law did apply in such a case, the Court noted that the Directive should be interpreted to have 'a particularly broad territorial scope'.[61] The Court also held that the right to delete data under the EU Data Protection Directive applies to the results of Internet search engines (popularly referred to as the 'right to be forgotten').[62]

The influence of *Kadi* can be seen in the self-referential style of the *Google Spain* judgment, in which the Court does not even mention the European Convention on Human Rights, the jurisprudence of the European Court of Human Rights, or any international human rights instruments. By contrast, in his opinion Advocate-General Jääskinen had recognised the implications of the case for the global Internet,[63] an approach that the Court did not refer to and thus impliedly rejected. This is also demonstrated by the fact that the Court favoured data protection rights over the rights of

---

58 Digital Rights Ireland, para. 68.

59 See EU Data Protection Directive, Article 28.

60 Case C-131/12 (13 May 2014).

61 *Id.*, para. 54.

62 *Id.*, paras. 89–99.

63 See Opinion of Advocate General Jääskinen, Case C-131/12, 25 June 2013, paragraph 31, mentioning the need in the case to strike 'a correct, reasonable and proportionate balance between the protection of personal data, the coherent interpretation of the objectives of the information society and legitimate interests of economic operators and Internet users at large'. See also regarding the implications of the case for the Internet, Ausloos, J., "European Court Rules against Google, in Favour of Right to be Forgotten", 13 May 2014, available online at <blogs.lse.ac.uk/mediapolicyproject/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten/> (accessed 1 July 2014); Jerker B. Svantesson, D., "Google court ruling creates a more forgetful Internet", 14 May 2014, available online at <theconversation.com/google-court-ruling-creates-a-more-forgetful-internet-26696> (accessed 1 July 2014).

Internet users,[64] and did not refer to the right to transfer data 'regardless of frontiers' that is protected both by international human rights law[65] and the EU Charter of Fundamental Rights.[66] *Google Spain* thus seems to mark a new era in which the CJEU applies to data processing on the Internet the pronouncements made in the *Kadi* judgment on the autonomy and primacy of EU data protection rights.

An upcoming decision by the CJEU may develop the themes dealt with in *Digital Rights Ireland* and *Google Spain* even further. On 18 June 2014 the Irish High Court stated that it would refer a question to the CJEU in the case *Schrems v. Data Protection Commissioner*,[67] which involves a challenge by an Austrian student to the transfer of personal data to the US by Facebook under the EU-US Safe Harbor scheme. While the exact wording of the question(s) to be referred to the CJEU had not yet been published when this article was finalised, it seems that they will involve whether the European Commission's adequacy decision of 2000 creating the Safe Harbor should be re-evaluated in light of widespread access to data by US law enforcement, and whether the DPAs should be allowed to determine whether the Safe Harbor provides adequate protection.[68] The High Court in the *Schrems* case criticised the Safe Harbor and data access by law enforcement in the US as failing to provide oversight 'carried out on European soil',[69] which seems inspired by paragraph 68 of the *Digital Rights Ireland* judgment.

III.3. Data protection standards and applicable law

The extraterritorial application of data protection law currently fulfil much the same function as would an international legal framework, i.e., it extends legal protection to the processing of the personal data regardless of their location. This can be seen in the case of EU data protection law, which often applies to data processing outside the EU, and which also includes restrictions on transborder data flows that require data processing in third countries to be conducted under EU data protection standards.[70]

An effective global legal framework for data protection thus requires clarity about rules of applicable law. In the author's experience, bodies drafting transnational data protection rules are reluctant to deal with the topic of applicable law because of its complexity and the fear of unintended consequences,[71] and thus far, the EU Data Protection Directive is the only international data protection instrument to contain rules on applicable law.[72] There is thus no accepted international framework for applicable law rules as they relate to data protection.

---

64 See Google Spain, paragraph 81, stating that the data subject's rights protected by Articles 7 and 8 of the Charter of Fundamental Rights 'override, as a general rule, that interest of internet users …'.

65 UDHR, UN GA Res 217 A(III), Article 19; ICCPR, 999 UNTS 171, 1966, Article 19(2).

66 See Article 11 of the Charter, which states: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.

67 2013 No. 765JR, 18 June 2014.

68 *Id.*, paras. 71 and 84.

69 *Id.*, para. 62.

70 See Kuner, C., *Transborder Data Flows and Data Privacy Law*, Oxford, Oxford University Press, 2013, 125–129.

71 With regard to the failure of the Council of Europe Convention 108 to include clear rules on applicable law, see Bygrave, *supra* nt. 5, locations 2057–2058 (Kindle edition).

72 I*d.*, location 2428 (Kindle edition).

III.4. The increasing insularity of EU law

The recent judgments of the CJEU cited above (in particular *Kadi* and *Google Spain*) reflect an increasing concern for the autonomy of EU law and a self-referential style that carry the risk of a growing insularity.

This is also reflected in the lack of options in EU data protection law for granting legal recognition to non-EU data protection standards. The Directive recognises non-EU standards only in line with a formal adequacy determination by the European Commission, as described above. The Regulation proposed in 2012 fails to include a provision explicitly requiring the Commission to take into account the enactment by third countries of regional and international instruments (for example, Council of Europe Convention 108) when assessing the adequacy of protection.

The increasing insularity of EU data protection law can also be seen in the involvement of the EU in international policymaking bodies like the Council of Europe and the OECD. Over the last few years, it seems that the EU's priority in participating in the work of such organisations is to emphasise the need to finalise enactment of the proposed Regulation, rather than to further the adoption of a global legal framework for data protection.[73]

The recent judgments of the CJEU also demonstrate the tension between the promotion of EU data protection law and the furtherance of other important fundamental rights on a global basis. The Internet enables communication and the dissemination of information across borders, which brings great cultural, economic, and social benefits to individuals in the EU. If access to Internet services becomes fragmented along regional or national lines, then these benefits will be diminished. The judgment in *Google Spain* may cause Internet search results to be presented to individuals in the EU in a different way than they are in other regions.[74] In fact, the judgment has already led to controversy concerning the effect of deleting links to news stories on a regional basis.[75] The Snowden revelations are also strengthening the interest in initiatives such as a "Schengen for data" that would provide incentives to store the data of European companies on servers located within the EU.[76]

---

[73] Based on the author's experience as an observer for the International Chamber of Commerce (ICC) in the data protection work of the Council of Europe, and as a consultant for the OECD.

[74] See Ahmed, M., "Google in fight to stop global removal of sensitive links", *Financial Times*, 23 July 2014, available online at <ft.com/intl/cms/s/0/f3dfc9e4-127b-11e4-93a5-00144feabdc0.html?siteedition=intl#axzz38KKenC25> (accessed 23 July 2014), indicating that the DPAs have been pressing Google to interpret the *Google v. Spain* decision as requiring that links expunged from Google's European search engines should also be removed from its website google.com.

[75] Ball, J., "EU's right to be forgotten: Guardian articles have been hidden by Google", 2 July 2014, available online at <theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google> (accessed 8 July 2014). See also Article 29 Working Party, "European DPAs meet with search engines on the 'right to be forgotten'", 25 July 2014, available online at <ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140725_wp29_press_release_right_to_be_forgotten.pdf> (accessed 27 July 2014).

[76] See "Atos CEO calls for 'Schengen for data'", available online at <thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html> (accessed 6 July 2014); "Ein Internet nur für Deutschland", *Frankfurter Allgemeine Zeitung*, 10 November 2013, available online at <faz.net/aktuell/wirtschaft/netzwirtschaft/plaene-der-telekom-ein-internet-nur-fuer-deutschland-12657090.html> (accessed 6 July 2014).

IV. Conclusions

IV.1. The pluralist nature of global data protection policymaking

The EU's activities on the international stage have been marked by tension between efforts to strengthen the international legal framework for data protection on the one hand, and the increased emphasis given to the fundamental right of data protection under EU law and the autonomous nature of EU law on the other hand. These latter points were also strengthened by the *Kadi* judgment, where the CJEU's reasoning emphasised 'the separateness and autonomy of the EC from other legal systems and from the international legal order more generally, and the priority to be given to the EC's own fundamental rules'.[77]

This tension reflects the pluralist nature of the international legal order.[78] In a pluralist view, the presence of various conflicting norms is a normal situation when there is a lack of a hierarchical legal structure that can provide an overall, authoritative governance framework.[79] The EU's apparent decision that the best way to develop data protection at a global level is to promote and apply its own data protection law extraterritorially could have either positive or negative consequences for the further global recognition of data protection rights, depending on the direction which global developments take

> [I]f each instrument takes positive steps to converge with the others, creating in essence a single international regulatory framework, international governance of data privacy would benefit from an unexpected gift. However, if on the contrary, each model decided to further its own purposes and follow its own path, one more obstacle to the creation of a single regulatory framework would be erected by the release of yet another generation of diverging approaches.[80]

The same impediments to the adoption of an international legal framework that existed in 2009 still exist today, namely the lack of an international organisation to oversee the work; cultural and legal differences between various systems of data protection law; and uncertainty about how such standards could be implemented at the national level.[81] However, even if 'the short-term chances of extensive harmonization are slim',[82] this should not impede work towards greater harmonisation and interface between systems, and dialogue concerning the conflicting attitudes towards data protection may serve as the basis upon which a global framework can gradually be constructed. All this is consistent with a pluralist view of data protection at a global level.

At present, the Council of Europe Convention 108 presents perhaps the best treaty-based possibility for the adoption of an international data protection framework.

---

77 de Búrca, *supra* nt. 50, 23.

78 Regarding pluralism as a normal feature of the international legal order, see UN International Law Commission, "Fragmentation of International Law: Difficulties arising from the Diversification and Expansion of International Law, Report of the Study Group of the International Law Commission finalized by Martti Koskenniemi", UN DOC A/CN.4/L.682, 13 April 2006, available online at <legal.un.org/ilc/documentation/english/a_cn4_l682.pdf> (accessed 3 July 2014), 248.

79 See Krisch, N., "The pluralism of global administrative law", *European Journal of International Law*, vol. 17, ed. 1, 2006, 247–278, 278.

80 De Hert and Papakonstantinou, *supra* nt. 33, 323.

81 Bygrave, *supra* nt. 5, location 6167 (Kindle edition).

82 *Id.*, location 6167–6168 (Kindle edition).

Convention 108 has the advantage that it offers a high level of protection, and is based on existing EU data protection law, which automatically makes it interesting for those States that have adopted the EU approach. At the same time, it requires detailed national implementation, thus being flexible enough to accommodate a variety of national differences. In some respects Convention 108 thus resembles a model law of the type promulgated by international organizations such as UNCITRAL, i.e., it sets forth high-level rules while leaving the details up to local implementation. The advantages (flexibility) and disadvantages (the potential for lack of harmonisation) are also similar to those of a model law. Unfortunately, it seems that the EU (which wields great influence within the Council of Europe) is unwilling to tolerate finalisation of the modernisation process for the Convention 108 until its proposed General Data Protection Regulation is adopted.

It would be useful for the development of global data protection standards if the international community would devote greater efforts to mapping areas of convergence between standards in different legal systems. Greater mutual understanding about the different cultural and legal approaches to data protection around the world would help create the conditions for eventual adoption of an international framework. Academic institutions should also devote greater attention to the area of comparative data privacy law than is now the case.

A good example of such an initiative is the "referential" that has recently been released regarding the use of binding corporate rules (BCRs) in the EU and corporate binding privacy rules (CBPRs) in the APEC countries.[83] The referential is a document matching the legal requirements for BCRs and CBPRs, which are mechanisms recognised under EU data protection law and the APEC Privacy Framework respectively to allow corporate groups to transfer personal data across borders based on their having implemented certain data protection measures within all members of the group. It is intended to serve as a checklist for companies interested in matching the requirements in both systems, and thus can help lead to gradual accommodation between them, without seeking to produce legal harmonisation.

Another initiative aimed at building bridges between different data protection systems is the "Privacy Bridges" project, which is a group of experts from the EU and the US who are drafting 'a framework of practical options that advance strong, globally-accepted privacy values in a manner that produces interoperability and respects the substantive and procedural differences between the two jurisdictions'.[84]

---

[83] Article 29 Working Party, 'Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents', 27 February 2014, available online at <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf> (accessed 30 September 2014).

[84] MIT Information Policy Project, MIT Information Policy Project and University of Amsterdam Institute for Information Law launch EU-US Privacy Bridges Study Project, 5 May 2014, available online at <ipp.mit.edu/news/mit-information-policy-project-and-university-amsterdam-institute-information-law-launch-eu-us> (accessed 30 September 2014). The author is a member of the project group.

IV.2. Areas for EU action

The following are three areas in which the EU's approach to the international dimension of data protection could be improved:

Considering the impact of EU policymaking on third countries: Many of the third countries that have enacted legislation based on EU data protection law are developing countries with limited resources, and enacting a legal framework for data protection and all it entails (for example, setting up an independent DPA) can be a considerable burden.[85] The fact that the EU promotes the adoption of its data protection law to third countries means that it has a special responsibility towards them. Indeed, the EU's proposed reform would in effect require many third countries that have already enacted EU-based models to make wide-ranging changes to their data protection legislation, and substantial investments in their data protection infrastructure, in order to have a chance of being found adequate by the EU.[86]

The EU is obligated to advance human rights and the rule of law in its relations with third countries,[87] which includes the promotion of data protection standards. It is also obligated to 'promote multilateral solutions to common problems',[88] which should involve more than simply motivating other States to adopt EU data protection law and then leaving them to their own devices. The EU should thus implement measures to consider the effect on third countries of its data protection rules, and to provide a mechanism for them to obtain information about the effects of such changes. Dozens of smaller and less powerful third countries are affected by EU data protection policymaking, but may have no resources to make their voices heard in Brussels. The author has often received questions from third country representatives about EU law-making initiatives in data protection, so interest on their part certainly exists.

It is becoming increasingly recognised that States or international organisations (like the EU) may have an obligation to account for their actions to foreign stakeholders; examples already exist in areas such as world trade law and environmental law.[89] This does not mean that the EU should sacrifice the interests of its own citizens;[90] indeed, doing so would be legally impossible given the autonomous nature of EU and the primacy of fundamental rights in the EU legal order. However, the EU could at least consult with third countries, gather input from them, and provide them with basic information about EU data protection policymaking, without adversely affecting the interests of EU individuals.

---

85 See, e.g., Madhub, D., "The pioneering journey of the Data Protection Commission of Mauritius", *International Data Privacy Law*, vol. 3, ed. 4, 2013, 239–243.

86 See European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), available online at <europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> (accessed 30 September 2014), which would cause adequacy decisions issued by the European Commission to expire after five years, unless they have been amended, replaced or repealed by the Commission.

87 See Consolidated version of the Treaty on the Functioning of the European Union (TFEU), *supra* nt. 46, Article 21.

88 *Ibid*.

89 See Benvenisti, E., "Sovereigns as trustees of humanity: on the accountability of states to foreign stakeholders", *American Journal of International Law*, vol. 107, ed. 2, 2013, 295–333, 319–320.

90 *Id.*, 300.

The European Commission proposal for a General Data Protection Regulation foresees a duty of cooperation and information of the Commission and the DPAs with regard to international developments,[91] but this should be made more concrete. For example, a provision could be included in the Regulation requiring the Commission to establish an Internet portal with information on data protection developments with particular relevance to third countries, to hold regular consultations with them, and to establish an advisory board of third country representatives who would give feedback on the impact of EU data protection law in their countries and regions.

Setting jurisdictional boundaries: The *Digital Rights Ireland* judgment demonstrates that the CJEU will apply the fundamental right to data protection broadly in a territorial sense.[92] Furthermore, in the *Google Spain* case the Court affirmed the applicability of EU data protection law to data processing on servers located in a third country, while conspicuously failing to endorse its holding in *Lindqvist* that EU data protection law should not be interpreted to apply to the entire Internet. The *Google Spain* judgment thus undermines the Court's holding in *Lindqvist*.

The EU seems to have decided to further the global protection of personal data by applying its own standards extraterritorially, rather than moving forward with a new set of standards on an international level. However, the territorial extent of data protection rights under EU law needs to be clarified.[93] Limits to the broad territorial scope of EU data protection law must exist, if it is not to become a system of universal application that applies to the entire world. The CJEU should clarify the geographic limits of EU data protection law, and in doing so should take into consideration the points that Advocate-General Jääskinen had mentioned in his opinion in the *Google Spain* case, in particular the objectives of the information society and the legitimate interests of Internet users.

Providing a better interface with other systems: In the absence of a global data protection framework, different regional standards must be able to co-exist. This would be in the EU's interest, as it would provide an incentive for other regions to move their systems closer to that of the EU. At present, EU law only provides for a possible "adequacy" decision being formally adopted by the European Commission. However, such a decision is based on the third country essentially adopting the EU data protection system, and is thus less an interface than a confirmation that the third country has adopted a system substantially similar to EU law. The procedure for an adequacy decision is cumbersome, and few third countries have received one,[94] so that it seems insufficient as a method of international interface.

There are various possibilities for such an interface. The most wide-ranging one would be for EU law to provide full legal recognition to data protection standards in other regions; this seems to be what the White House means by "international interoperability" between the EU and the US in the paper proposing a consumer data privacy framework

---

91 See General Data Protection Regulation, *supra* nt. 39, Article 45.

92 The author knows of influential EU policymakers who share this interpretation of that case.

93 See *EJIL Talk*, Kuner, C., "Extraterritoriality and the fundamental right to data protection", 16 December 2013, available online at <ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> (accessed 30 September 2014); Milanović, *supra* nt. 27.

94 As of July 2014, thirteen such decisions had been adopted in the sixteen years since the Directive came into force. See European Commission, *Commission Decision on the Adequacy of the Protection of Personal Data in Third Countries*, available online at <ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm> (accessed 30 September 2014).

that it published in 2012.[95] However, the political difficulties for the EU to adopt such a system with regard to data protection seem considerable.[96] In addition, the *Kadi* judgment puts into question the possibility of fully recognising a data protection system that does not incorporate EU concepts of fundamental rights (such as that of the US).

However, some room still remains for accommodation between EU data protection law and standards in other regions. From an EU perspective, such accommodation should be possible as long as such standards provide an 'adequate level of protection'.[97] The key challenge here will be to define the core or essential elements of data protection on an international scale. Data protection law contains a number of legal obligations, some of which are central to its nature as a fundamental right while others are not.[98] The EU Charter of Fundamental Rights refers to the "essence" of fundamental rights and freedoms,[99] and explicitly mentions the requirement that data be processed based on consent or some other legal basis, the rights of access and rectification, and control of data protection rules by an independent authority.[100] These can thus be seen as the essential elements of the fundamental right to data protection under EU law. The way that these elements are elaborated in detail to promote convergence in privacy standards between different regional and national systems of regulation would depend on international negotiations that are beyond the scope of this article.

Even if a system does not qualify as fully "adequate" under the EU standard, a narrower level of recognition could still be provided to it. For example, the enactment by a State of Council of Europe Convention 108 may by itself not be sufficient to ensure that it offers "adequate protection", but granting some lesser degree of recognition to States that have enacted it (i.e. considering them as having moved at least part of the path towards adequacy) would help build bridges between the EU system and States that enact the Convention (particularly States outside the EU). At present enactment of the Convention is regarded informally as one indication of potential adequacy,[101] but this is not formally set forth in the Directive.[102] The proposal of the European Commission for a General Data Protection Regulation also contains no mention of the Convention 108 or its interaction with EU data protection law, but the Council of the European Union in its deliberations on the Regulation has proposed adding a provision requiring the Commission to take into account a third country's accession to the Convention when

---

[95] White House, *Consumer Data Privacy in a Networked World*, February 2012, available online at <whitehouse.gov/sites/default/files/privacy-final.pdf> (accessed 30 September 2014).

[96] See Schwartz, P., *Differing privacy regimes: a mini-poll on mutual EU-U.S. distrust*, 22 July 2014, available online at <privacyassociation.org/news/a/differing-privacy-regimes-a-mini-poll-on-mutual-eu-u-s-distrust/> (accessed 30 September 2014).

[97] See Kokott, J. and Sobotta, C., "The Kadi case—constitutional core values and international law—finding the balance", *European Journal of International Law*, vol. 23, ed. 4, 2012, 1015–1024, 1018, stating that the reason for the CJEU's approach in the Kadi case was that the UN Security Council resolution at issue did not provide sufficient protection for fundamental rights.

[98] See European Data Protection Supervisor, Hustinx, P., *Concluding Remarks made at 3rd Annual Symposium of the European Union Agency for Fundamental Rights*, Vienna, 10 May 2012, available online at <secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-05-10_Speech_Vienna_EN.pdf> (accessed 30 September 2014).

[99] Article 52(1).

[100] *Id.*, Articles 8(2)–(3).

[101] Article 29 Working Party, "First orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy" (WP 4, 26 June 1997), 8–9.

[102] See EU Data Protection Directive, Recital 11, stating that the provisions of the Directive 'give substance to and amplify' those contained in Council of Europe Convention 108.

assessing adequacy.[103] Greater use could also be made of adequacy decisions that apply only in specific industries or sectors.

IV.3. Final thoughts

The challenge for the EU with regard to development of a global data protection framework is to promote strong standards at the international level, while avoiding the *Kadi* Court's approach of 'withdrawing into one's own constitutional cocoon, isolating the international context and deciding the case exclusively by reference to internal constitutional precepts'.[104] Taking steps to deal with the three issue mentioned herein would go some way to providing an interface with other legal systems that could help to develop international standards gradually, without weakening the fundamental right to data protection under EU law.

The EU should also recognise that, if it wants its data protection law to be the "de facto standard for the world", then it has certain responsibilities towards other States that adopt it, particularly those in the developing world. Recognition of such responsibilities would ultimately be in the EU's interest, since it would provide additional incentives for other countries to adopt EU data protection law.

The EU should thus be accountable both to maintain its high level of data protection and comply with its obligations under EU fundamental rights law, and to provide sufficient interfaces to other data protection systems. Only this mixture of respect for fundamental rights and flexibility towards the variety of data protection systems that exist around the world can provide the conditions under which an international legal framework for data protection can eventually develop.

*

[103] Council of the European Union, Note from the Presidency to the Working Party on Information Exchange and Data Protection, no. 11028/14, 30 June 2014, Article 81a.

[104] EJIL Talk, Weiler, J., "Editorial: EJIL Vol. 19:5", available online at <ejiltalk.org/letters-to-the-editor-respond-to-ejil-editorials-vol-195/> (accessed 30 September 2014), describing the approach of the CJEU in the *Kadi* judgment.

USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining?

Joanna Kulesza*

Keywords
PRIVACY; HUMAN RIGHTS; INTERNET GOVERNANCE; DUE DILIGENCE; JURISDICTION

Abstract
The paper covers the political and legal consequences of US deployed extensive cyber surveillance program, usually referred to with the codename PRISM. The author identifies the significant transnational legal challenges for privacy protection originated by US cybersecurity policy and the steps taken by other states aimed at limiting its consequences harmful to individual privacy. The author covers varying reactions to US-imposed privacy intrusions, from Brazil's plans to withdraw from the global network to some states' suggestions of holding Washington internationally responsible for violating the International Covenant on Civil and Political Rights. The paper's focus however is on the European personal data protection thus far not providing effective transnational protection of privacy, primarily through the strongly criticised and ineffective EU-US Safe Harbor arrangement. The EU personal data reform, approved by the European Parliament in March of 2014, seems the most significant consequence of mass privacy violations committed by the US National Security Agency and its agents.

The 2012 proposed Data Protection Regulation, which, together with the new personal data Directive**,** are to replace the 1995 Data Protection Directive 95/46/EC put strong emphasis on the effectiveness of transboundary privacy protection, although cover also many other significant changes, such as introducing the right to be forgotten or centralising the personal data protection decisions thus-far distributed among national Data Protection Authorities, often varying in their interpretations of community law. The reform is to oblige all companies, regardless of their country of incorporation, to meet EU privacy laws as it introduces high financial responsibility for those who fail to do so, making it a trigger for a significant change in the way the online markets operate.

The European approach seems significant for the entire international community not only because European citizens are an important element of the online markets, but also because personal data protection as a tool for safeguarding individual privacy has been adopted in over 100 out of the roughly 190 world's countries. Including an element of transnational data protection in EU law is therefore certain to influence the approach to privacy in other continents.

I. Introduction

The paper covers the political and legal consequences of US-deployed extensive cyber surveillance, usually referred to as PRISM. The author identifies the significant transnational legal challenges to privacy protection originated by US national security policy and steps taken by other States aimed at limiting its consequences for individual privacy right. The paper discusses varying reactions to US-imposed privacy intrusions, from Brazil's plans to withdraw from the global network to suggestions of holding

* Joanna Kulesza, Assistant Professor of Public International Law, University of Lodz, Poland.

Washington internationally responsible for violating the International Covenant on Civil and Political Rights and the universal human right to individual privacy. The paper's focus is on the European personal data protection laws thus far not providing effective transnational privacy protection, primarily through the strongly criticised and ineffective EU-US Safe Harbor arrangement. The EU personal data reform, approved by the European Parliament in March 2014, seems the most significant consequence of mass privacy violations by the US National Security Agency (NSA) and its agents. Focal to the reform, the 2012 proposed General Data Protection Regulation (GDPR) puts strong emphasis on the effectiveness of transboundary privacy protection. The reform aims to oblige all companies operating on EU citizens' data, regardless of their country of incorporation, to meet EU privacy laws.

This paper is an attempt to verify how effective the new EU regime is in resisting US cyber surveillance attempts. The author covers the personal data protection derogations included in the GDPR and turns to existing international business law standards as catering for the need to enforce universal privacy safeguards.

II. US "Signals Intelligence" Laws—the Origins of the Problem

Sixth of June 2013 was the day that proved conspiracy theorists right. Simultaneous publications by the New York Times, The Guardian and Der Spiegel on secret US surveillance programs disclosed multiannual and versatile electronic espionage of domestic and foreign individuals by the NSA.[1] The publications were based on top secret information, revealed to the journals by an ex-NSA contractor, Edward Snowden and proved the validity of long-lasting suspicions of US running its unique Panopticon,[2] operating under the code name PRISM, an abbreviation originally used by the NSA for its Planning Tool for Resource Integration, Synchronization, and Management.[3] It describes the use of three key surveillance programs, all serving the same purpose of collecting and automatically synthesising information about users of telecommunication services, including those obtained from Internet service providers. While UPSTREAM was the program used for collecting data from public and private networks through international fiber-optic connections and Internet Exchange Points, the XKeyscore was an analytic system for buffering and retaining data from hundreds of websites and servers

---

1 Washington Post, Gellman, B. and Poitras, L., *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, 7 June 2013, available online at <washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html> (accessed 28 October 2014); The Guardian, Greenwald, G. and MacAskill, E., *NSA Prism program taps in to user data of Apple, Google and others*, 7 June 2013, available online at at <theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (accessed 27 October 2014).

2 The term Panopticon was first used by 18th century English philosopher Jeremy Bentham to describe a prison building whose architecture would enable one-man surveillance of all inmates without them being aware of being watched at a given time. The very possibility of being watched resulted in inmates obeying the rules of the facility, not wanting to risk punishment. With time the term came to signify comprehensive, secret surveillance imposed by authorities.

3 The 2013 publications confirmed previous information on US cyber surveillance, provided by whistleblowers in 2005, see, e.g., New York Times, Risen, J. and Lichtblau E., *Bush Lets US Spy on Callers Without Courts*, 16 December 2005, available online at <nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0> (accessed 27 October 2014).

around the world while combining it with data from other sources, such as diplomatic and intelligence resources at US's disposal.[4] Its key function was to index such information using IP or e-mail addresses, phone numbers, cookies, usernames, search terms or location data as well as metadata retained by websites.[5] Finally, BULLRUN was used to break encryption safeguarding data stored on resources reached by the two other programs through, for example, backdoors installed in software and hardware delivered by companies operating under NSA contracts.

Those three tools have technically enabled the NSA to obtain, store and analyse information on US nationals and foreigners. The legal basis for their operation was the Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008,[6] which enhanced the powers granted to the NSA by the 2001 USA PATRIOT Act.[7] When discussing the FISAA, two elements of the unique US perception of the right to privacy must be mentioned: lack of privacy protection for data provided to the government by third parties, such as banks or telecommunication companies (the so-called third party doctrine) and the varied approach to the protection of US citizens as compared with "non-US persons", whose data was unprotected by US law. The right to privacy is granted to all US citizens in the Fourth Amendment to the US Constitution and warrants them freedom from 'unreasonable searches and seizures' making any privacy invasion subject to a judicial warrant issued upon 'a probable cause, describing the place to be searched'.[8] As per 1970s US case law, this protection does not apply to private information about an individual obtained not directly from him, but from a third party, such as a bank or a telecommunication company (third party doctrine).[9] This derogation of privacy protection was extended by the already mentioned 2001 USA PATRIOT Act, which allowed security authorities to access companies' business records. After numerous protests from civil society and privacy activists USA PATRIOT Act was amended in 2006 to allegedly limit such privacy interferences, covering access to only "relevant" information. This broad interpretative clause however proved ineffective, especially with the introduction of the 2008 FISAA. Further derogations resulted from section 702 FISAA, allowing the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Surveillance Court of Review (FISCR) the discretion in interpreting the Act, and deciding on what "relevant" information is. The scope of such information was set very broadly, as based on the "three hops" rule (more recently limited to "two

---

4 European Parliament, Bowden, C., The US National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and Their Impact on EU Citizens' Fundamental Rights, 2013, available online at <europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf> (accessed 27 October 2014) (EP 2013).

5 *Id.*, 14.

6 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 6304, United States of America, 10 July 2008, Chapter 36 Section 1801 *et seq.*, available online at <congress.gov/110/plaws/publ261/PLAW-110publ261.pdf> (accessed 27 October 2014) (FISAA).

7 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Public Law 107-56, 115 Stat. 277, United States of America, 26 October 2014, available online at <gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf> (accessed 27 October 2014) (USA PATRIOT Act)

8 The Constitution of the United States, Amendment IV, available online at <constitutioncenter.org/media/files/constitution.pdf> (accessed 27 October 2014).

9 See, e.g., the recent case of *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012).

hops").[10] As per an NSA representative's explanation, the decision on whether data relating to a certain individual is to be collected depends on the possibility to link his telephone number with other numbers connected with a terrorist activity within "three hops". This connection is made based upon the definition of "foreign intelligence information", subject to NSA's inspection. The FISAA definition of such information covers all information relating to, and if concerning a United States person, necessary for the United States to protect itself against foreign attacks or "hostile acts", sabotage, terrorism, proliferation of weapons of mass destruction or clandestine intelligence activities.[11] It also covers 'information with respect to a foreign power or foreign territory' relating to or, if concerning a US person, 'necessary for the purpose of' national defense, protecting US security or conducting foreign affairs of the US. Such a definition clearly indicates two groups of subjects regarding whom information may be processed, giving weaker protection to "non-US persons", while no definition of a "US person" is to be found within the FISAA. As per the explanations provided by the NSA, the constitutional privacy protection is understood to be granted only to US citizens.[12] While their information is to be collected only when "necessary" for the purposes of US security and foreign policy, data on non-citizens can be compiled and analysed when it only "relates to" those, very broadly designed, terms. The decisions on the relevance of such data are made by the NSA and require judicial oversight only when referring to "US persons". There is no judicial supervision requirement for accessing the information of non-US persons, since neither FISAA nor the US Constitution is applicable to them. As explained by NSA and confirmed by the FISC the national guarantees were applied only to those covered by US law, while none of its acts provide for any protection of foreign individuals.[13] As explained in detail below, the US does not recognise the direct applicability of international treaties, binding upon them and constituting such a right. Should the individual under surveillance be a US citizen, a court order for their surveillance would be issued. Such an order, directed at a service provider, required them to promptly provide to US authorities 'all information, facilities, or assistance', including not just traffic data or communication content, but also cryptographic tools used to safeguard individual communication.[14] A year after the PRISM revelation and despite some presidential actions, such as the Presidential Policy Directive/PPD-28, extending minimal safeguards onto non-US citizens, the protection granted to them is still nowhere near sufficient.[15] Effectively FISAA allows the NSA to intercept "non-US persons" communications without judicial oversight or a right to obtain information about their data being collected, even though the right to privacy, recognised within international human rights law, its treaties and customary practice, discussed in detail below, disallows for any blanket surveillance and unjustified invasions of privacy.

---

[10] The Guardian, Timm, T., *The House's NSA bill could allow more spying than ever. You call this reform?*, 25 March 2014, available online at <theguardian.com/commentisfree/2014/mar/25/house-nsa-bill-end-bulk-collection-act-reform> (accessed 27 October 2014).

[11] Section 702 FISAA.

[12] CBS News, Trowbridge, A., *NSA spying: Ally anger justified?*, 3 July 2013, available online at <cbsnews.com/news/nsa-spying-ally-anger-justified/> (accessed 27 October 2014).

[13] *Ibid*.

[14] Section 702 FISAA.

[15] The White House, *Presidential Policy Directive – Signals Intelligence Activities*, 17 January 2014, available online at <whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (accessed 27 October 2014).

III. PRISM and International Law—Has US Violated the Human Right to Privacy? And with What Consequences?

The first document of international human rights law is the 1948 Universal Declaration on Human Rights.[16] This non-binding compromise was easy to achieve just a few years after the greatest horrors in human history unfolded on the frontlines of World War II. Yet completing a binding treaty, expressing the very same ideals, took the international community almost twenty more years, as States agreeing on the notions of individual rights, such as privacy, free speech or property, saw differently the scope and implementation of each of them. The 1966 International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic Social and Cultural Rights (ICESCR) introduced hard law obligations for different categories of innate human liberties, leaving the detailing of each of them up to State practice and international jurisprudence.[17] Privacy holds a well-established place in the human rights catalogue, with Article 12 UDHR and Article 17 ICCPR granting every individual freedom from 'arbitrary interference' with their 'privacy, family, home or correspondence' as well as from any 'attacks upon his honor and reputation', placing privacy among the catalogue of personal rights known to every national legal system, yet perceived differently. While the very term "privacy" is not defined within the convention, the UN Human Rights Committee (HRC) provided detailed guidelines on the scope of privacy protected by international law, in particular when discussing the thin line with State sovereignty, security and surveillance.[18]

As per international law, confirmed by the interpretations and jurisprudence accompanying the ICCPR, privacy right must be safeguarded with national laws protecting individuals from 'arbitrary or unlawful' interferences or attacks upon it.[19] National authorities are therefore obliged to set limits on privacy invasions executed by themselves or third parties, although the two crucial human rights document differ by one significant element, defining it. The non-binding UDHR includes a limitative clause for all rights contained therein, in Article 29 paragraph 2 it surrenders the exercise of all rights and freedoms subject to limitations determined by law 'solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society'. The ICCPR includes no such general restraint, nor one aimed directly at privacy, even though it does contain explicit limitations on other freedoms, such as the one in Article 19 paragraph 2, referring to the freedom of expression. The latter

---

[16] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, UNGA Res 217 A (III), (UDHR).

[17] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, 999 UNTS 171 (ICCPR); UN General Assembly, International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, Treaty Series, 993 UNTS 3 (ICESCR).

[18] The Human Rights Committee (HRC) ought to be distinguished from the United Nations Human Rights Council (UNHRC) and the Commission on Human Rights. According to Article 28 of the ICCPR, the HRC consists of eighteen members, nationals of the States parties with recognised competence in the field of human rights and legal experience, who monitor the implementation of the ICCPR by its State parties. On the other hand the UNHRC is an inter-governmental body subsidiary of the UN General Assembly. It collaborates with the Office of the High Commissioner for Human Rights and aides the United Nations' engagement in special procedures. In 2006 the UNHRC replaced the United Nations Commission on Human Rights which carried similar functions.

[19] Article 12 UDHR; Article 17 ICCPR.

introduced a standardised three-steps test, which, even though its wording might be considered vague, sets minimal standards required from State parties agreeing to grant its subjects freedom of thought and communication.[20] Despite the fact however that Article 17 ICCPR is not accompanied by a limitative clause, the right to privacy is not to be considered an absolute one. As per the ICCPR practice and the HRC interpretations privacy may be subject to legal limitations as long as those meet the general standards present in human rights law and similar international treaties, just to mention Article 8 of the European Convention on Human Rights (ECHR),[21] which allows to restrict individual privacy with laws necessary in a democratic society for the protection of rights and freedoms of others.

The HRC confirmed this interpretation on various occasions, among which the 1988 General Comment No. 16 is most significant, as it paved the way for further elucidations.[22] Back in 1988, before the peak of the communications revolution brought about by the Internet,[23] the HRC stated that as per existing human rights norms, '[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited'.[24] It also approved the applicability of the general three-step test, recognised by the UDHR, for the right to privacy, granted by Article 17 ICCPR.[25] And so, the three steps test, as per this general human rights standard means that any limitation upon an individual right must be based on an act of law,[26] which ought to describe in detail the precise circumstances when privacy may be limited by authorities or third parties. The HRC specified that a decision on whether private information about an individual may be obtained must be made on a 'case-by-case basis',[27] emphasising that 'even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and reasonable in the particular circumstances', where "reasonable" means justified by those particular circumstances.[28] Moreover, not only does international law lay upon States the obligation to refrain from unjustified invasions of privacy, but it also includes their positive duty to protect individuals within their

---

[20] The three steps test means that any limitation upon an individual right must be based on an act of law, needs to be necessary in a democratic society and justified by one of the reasons named in the ICCPR, which include the protection of public order or the rights and freedoms of others.

[21] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, CETS 005 (ECHR).

[22] UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available online at <tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en> (accessed 24 November 2014).

[23] In 1991 the US National Science Foundation, funding the "Internet" research project allowed for setting up of the Commercial Internet eXchange (CIX), making the up-till-then purely academic network open to commercial use. The very same year the European Organization for Nuclear Research (CERN) introduced its "world wide web" protocol, significantly enhancing the commercial value of the network by making its operation more user-friendly. See Office of the Inspector General, National Science Foundation, *Review of NSFNET,* 1993, available online at <nsf.gov/pubs/stis1993/oig9301/oig9301.txt> (accessed 27 October 2014).

[24] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 28 December 2009, UN Doc. A/HRC/13/37 (A/HRC/13/37), 2.

[25] See above nt. 20.

[26] Human Rights Council, *supra* nt. 24, pt. 3, 1.

[27] *Id.*, pt. 8, 2.

[28] *Id.*, pt. 4, 1.

jurisdiction from privacy invasions committed by third parties by taking active steps to identify and mitigates such threats. The HRC emphasises that 'Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it'.[29]

As international espionage increased with the rising popularity of online communications and expanding war on terrorism, the HRC followed the initial 1988 General Comment with documents identifying and describing the interception of privacy and State security. In a 2009 report on the promotion and protection of human rights and fundamental freedoms and terrorism, it discussed the complicated equilibrium of State security and individual privacy.[30] According to the report, Article 17 ICCPR ought to be understood as allowing for 'necessary, legitimate and proportionate restrictions to the right to privacy' subject to 'a permissible limitations test'.[31] This test requires State authorities to 'justify why a particular aim is a legitimate justification for restrictions upon Article 17',[32] while identifying seven criteria of any such derogation. Consequently, a State may restrict individual privacy if such a restriction is 1) based on a provision of law; 2) does not interfere with the essence of the right; 3) is necessary in a democratic society; 4) is not subject to unfettered discretion; 5) is necessary to reach (rather than just aim at) one of those legitimate aims; 6) is proportionate; and 7) consistent with other ICCPR rights.[33] The HRC points to 6 principles which ought to guide best practice of any State when enforcing privacy restrictions. Those principles include 1) the principle of minimal intrusiveness, requiring States to ensure they have 'exhausted less-intrusive techniques before resorting to others';[34] 2) a data-minimisation principle, opting to refrain from obtaining information not necessary to meet a legitimate aim, even if it is technically possible to do so;[35] 3) the principle of purpose specification restricting secondary use, which declares the need to legally ensure data usage solely for the purposes for which they were initially gathered;[36] 4) the principle of oversight and regulated authorisation of lawful access, requiring States to ensure effective safeguards for the supervision of entities collecting and processing data;[37] 5) the principle of transparency and integrity, opting for openness and communication among States on their surveillance practices, and granting individuals the right to access information about themselves which has been collected by private and public bodies;[38] and 6) the effective modernisation principle, which encourages enhancing legislative and technological measures aimed at securing privacy, which include privacy impact assessments.[39]

---

[29] *Id.*, pt. 10, 2–3.
[30] A/HRC/13/37, *supra* nt. 24.
[31] *Id.*, 2.
[32] *Id.*, 1.
[33] *Id.*, para. 17.
[34] *Id.*, para. 49.
[35] *Ibid*.
[36] *Id.*, para 50.
[37] *Id.*, paras. 51–53.
[38] *Id.*, paras. 54–55.
[39] *Id.*, para. 57. Privacy impact assessments were recently introduced as an obligatory security measure ensuring privacy within the EU data protection reform, discussed below. For a detailed discussion on privacy and other human rights protection in the age of the information society see: The Jean Monet Center for International and Economic Law and Justice, Kulesza, J., *Protecting Human Rights Online - an Obligation of Due Diligence*, Jean Monnet Working Paper Series, 2014, available online at <jeanmonnetprogram.org/papers/papers14.html> (forthcoming).

The author of this 2009 HRC report, Martin Scheinin, given his expertise in the area, was asked to assess the US surveillance programs for the European Parliament once the Snowden revelations were published. In a 2013 statement for the European Parliament, he repeated his arguments on the validity of a universal human right to privacy subject to strict limitations, arguing that the US violated its international obligations and the right to individual privacy granted by Article 17 ICCPR of all those whose communications were intercepted by the NSA without judicial supervision.[40] He claims that

> the United States … have been involved, and continue to be involved, in activities that are in violation of their legally binding obligations under the International Covenant on Civil and Political Rights of 1966. … It includes a specific provision that prohibits unlawful or arbitrary interference with anyone's privacy[41]

emphasising the use of the term in the very text of the Covenant. He argues for an international complaint to be filed against the USA by other ICCPR member States as per Article 41 ICCPR (discussed in more detail in the following paragraph).

Martin Scheinin's interpretation, reflecting the European understanding of privacy, and strongly rooted in the HRC interpretation of Article 17 ICCPR, is, however, opposed by the US and international lawyers that support the US understanding of privacy. Eric A. Posner argues that no right to privacy can be identified in contemporary international law, hence no State or authority may be required to respect it, as the term is too ambiguous to carry any legal obligation. On the other hand national sovereignty carries with it an inherent "right to surveillance" granted to each State and exercised by authorities in European, American or Asian States alike.[42]

As much as the latter opinion seems unjustified in the light of the HRC body of work, it is a good reflection of the US perspective on privacy and its limits. Hence, it must be assessed that, while in Europe the right to privacy (as a universal standard defined by the HRC) raises no controversy, other legal cultures, as represented by the US, view the issue differently, regardless of whether their motivation is dogmatic, academic or a purely political one.

IV. Enforcing International Privacy Standards—Is International Human Rights Law Binding to the US?

Assuming that the HRC work serves as a litmus test on the existence of a human right to privacy, its scope and limits, one could credibly state that, through the implementation of the PRISM program, the US has violated international law. Such an assessment was confirmed by the HCR in its 2014 observations to US periodic review report.[43] Since the

---

[40] European Parliament, Scheinin, M., *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens*, 14 October 2013, available online at <europarl.europa.eu/document/activities/cont/201310/20131017ATT72929/20131017ATT72929EN.pdf> (accessed 24 September 2014) (LIBE Committee Inquiry statement).

[41] *Ibid*.

[42] Privacy & Civil Liberties Oversight Board, Posner, E. A., *Statement to the Privacy & Civil Liberties Oversight Board*, 14 March 2014, available online at <pclob.gov/Library/20140319-Testimony-Posner.pdf> (accessed 24 September 2014).

[43] OHCHR, Human Rights Committee, *Concluding observations on the fourth periodic report of the United States of America (HRC Observations)*, 23 April 2014, available online at

ICCPR is an international treaty, for its effectiveness, it requires ratification by a sovereign State, stating its willingness to give up parts of its sovereignty for the good of international cooperation. The US consented to such compromise when, in 1992, it ratified the ICCPR, adhering to the obligations and goals set in the treaty, yet having made significant reservations, limiting its effectiveness. The reservations, presented upon the ratification of the ICCPR, include, for example: denying the ICCPR a self-executing character, which effectively deprives all individuals under US jurisdiction of the possibility to demand protection for the rights named in the ICCPR directly from US authorities, unless such rights are reflected in national law.[44] The only obligation that the US did take upon itself, when it comes to meeting the ICCPR goals, is to implement the treaty through federal government, as well as State and local governments, making it their best efforts obligation to 'take appropriate measures for the fulfilment of the Covenant'.[45] Effectively, a right granted by the ICCPR and detailed by international jurisprudence and State practice, such as the right to privacy, named in Article 17 ICCPR, is not executable in the US, unless provided for by national law.

Moreover, although in its jurisdiction, the US denies the applicability of the ICCPR rights to individuals outside its territory, as noted by the HRC, such practice is contrary to the interpretation of Article 2 paragraph 1 ICCPR 'supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and State practice'.[46] The practice of affording also foreign individuals active privacy protection confirmed by the HRC serves as evidence for customary human rights law and is binding upon the US, despite the ICCPR reservations. The lack of recognition of individual rights granted by the ICCPR to non-US residents, whether those detained in Guantanamo or those under surveillance in Europe, is clearly in breach of well-established international law and practice.[47] The HRC's observations cover therefore the need for the US to 'interpret the Covenant in good faith, in accordance with the ordinary meaning to be given to its terms in their context, including subsequent practice, and in the light of the object and purpose of the Covenant, and review its legal position'.[48]

The HRC also addresses the non-self-executing reservation, calling upon the US to ensure 'effective remedies' against violations of the Covenant,

> including those that do not, at the same time, constitute violations of the domestic law of the United States of America, and undertake a review of such areas with a view to proposing to Congress implementing legislation to fill any legislative gaps,

eventually recommending the US to withdraw its reservations.[49] It is therefore clear that, according to the HRC, the US remains in violation of its international obligations as set within the ICCPR to which the US acceded in 1992. Moreover, the reservations might be

---

<tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en> (24 September 2014) (HRC Observations).

44 University of Minnesota, *US reservations, declarations and understandings, International Covenant on Civil and Political Rights*, 2 April 1992, pt. III(1), available online at <umn.edu/humanrts/usdocs/usres.html> (accessed 23 September 2014)

45 *Id.*, pt. II(5).

46 HRC Observations, *supra* nt. 43, pt. C.4, 2.

47 *Id.*, pt. C.4(a)–(c), 2.

48 *Id.*, pt. C.4(a), 2.

49 *Id.*, pt. C.4(c)–(d), 2.

considered as contrary to the very aim and scope of the convention and therefore inadmissible as per the law of treaties.[50]

In its observations on the US periodic report, the HRC directly addressed the privacy concerns raised by NSA.[51] Referring to the implementation of Section 215 of the USA PATRIOT Act and, 'in particular, surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act' it addressed their 'adverse impact on individuals' right to privacy'.[52] According to the HRC, the 'current oversight system of the activities of the NSA fails to effectively protect the rights of the persons affected' and the overall US practice grants persons affected by it 'no access to effective remedies in case of abuse'—a right well recognised by the ICCPR in Articles 2, 5(1) and 17.[53] The HRC therefore recommends that the US 'take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17'.[54] It refers directly to its body of work on Article 17 ICCPR, naming the need to introduce measures ensuring legality, proportionality and necessity of any privacy limitation, 'regardless of the nationality or location of the individuals whose communications are under direct surveillance'.[55] To meet that requirement, the US is directly obliged to ensure that any interference with the right to privacy or correspondence

> is authorised by laws that are
>
> (i) are publicly accessible;
>
> (ii) contain provisions that ensure that collection of, access to and use of communication s data are tailored to specific legitimate aims;
>
> (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorisation, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected; and
>
> (iv) provide for effective safeguards against abuse.[56]

Moreover, the HRC requires the US to reform its current oversight of the surveillance programs, ensuring its effectiveness. The US should therefore provide for 'strong and independent' judicial oversight over the authorising or monitoring of surveillance measures, to prevent abuses.[57] The 2014 Presidential Policy Directive PPD-28 fails to

---

[50] See Vienna Convention on the Law of Treaties, 1969, 1155 UNTS 331, Article 19, indicating that a State may formulate a reservation to a treaty unless 'the reservation is incompatible with the object and purpose of the treaty'. The convention does not however foresee a procedure of assessing which reservations are to be considered contrary thereto, leaving it up to the contracting States to hold other State parties to their obligations set per each treaty, as provided for by general international law norms.

[51] HRC Observations, *supra* nt. 40, pt. 22, 9.

[52] *Ibid*.

[53] *Id.*, pt. 22, 9–10.

[54] *Id.*, pt. 22, 10.

[55] *Ibid*.

[56] *Ibid*.

[57] *Ibid*.

meet that goal as it lacks judicial supervision over individual decisions on engaging bulk data collection.

Despite the fact that the US is in violation of its international law obligations, enshrined in the ICCPR and present in customary international law, the HRC recommendations remain by their very nature non-binding—the US is not legally obliged to introduce them, suffering only moral responsibility for the faults identified within the document, should they remained unattended to. This is not to mean, however, that there is no effective legal remedy against the US violations of international law.

V. PRISM Reactions—How Should States Protect Individuals from Privacy Invasions by Foreign Authorities?

The ICCPR provides for two complaint mechanisms, significant to the issue discussed herein.

The first is the procedure of individual complaints against State parties who fail to meet the treaty protection standards. As per the Optional Protocol, each individual within the jurisdiction, either territorial or effective, of a State party whose treaty rights have been violated has the right to address the HRC with a claim for assessing the potential violation and granting them an effective remedy against such infringement. Despite the limited success of the individual procedure, it is a direct remedy against human rights violations committed by ICCPR parties. The US never adopted the Optional Protocol, despite HRC recommendations.[58] The HRC disapproved of the way the US has implemented the ICCPR, emphasising the 'considerable limits' of its 'legal reach and practical relevance' in the US, as directly required by Article 2 ICCPR, demanding State parties to provide for domestic implementations of the guarantees provided for in the treaty.[59] With the US clearly failing to make the necessary changes, it stays in breach of international law by the deficient implementation of the ICCPR as well as international human rights law, created by the State practice and jurisprudence accompanying the treaty.

Since the US has not acceded to the Optional Protocol, nor does it indicate any plans to do so, individuals, whose privacy has been violated by the NSA, seeking compensation would need to base their claims on national US law and direct them at national courts with little chance of success, as the versatile privacy derogations in the USA PATRIOT Act and FISAA ensure extensive NSA freedom in limiting individual privacy.

Non-US persons aware of being under surveillance by the NSA,[60] however, might resort to national law in order to request protection against privacy violations they have suffered. Such claims may be directed not at the US but at local authorities who have failed to protect their residents, as international law requires State authorities not only to refrain from committing human rights violations, but also to take 'all necessary measures' to protect individuals under their jurisdiction from violations by third parties. Acting with

---

58 *Id.*, C.4(c), 2.

59 *Id.*, C.4, 2.

60 US laws do not provide for a right to information on the fact of being under surveillance, in line with many other national criminal procedure codes.

due diligence, State authorities are not obliged to effectively prevent all such violations, only to take all necessary steps to identify and mitigate such risks.[61]

Hence in the case of States whose residents have been under surveillance by the NSA, two different cases are to be analysed. As per the information available through official statements and media coverage, some States, such as the UK, have actively helped the US to gather and process information about individuals within their jurisdiction, or at least allowed for such information to be gathered by US agents. Other State authorities, such as those in Brazil, had little or no information on the private data of their subjects being stored. In the case of the UK and other US allies, their obligation to remedy the damages suffered by individuals is apparent. Individual claims against State authorities allowing for foreign surveillance without national, judicial supervision as well as against those who have failed to take all appropriate measures to identify and mitigate risks of such violations, may be based on national laws granting the right to privacy, meeting the international standards of legality and proportionality. Any national law reflecting the broad US derogations fails to meet the international standard discussed above and makes the State enforcing it liable under the ICCPR. Such States may be targeted with individual complaints under the ICCPR Optional Protocol by those individuals whose rights have been infringed. Yet should US allies in anti-terrorism surveillance not be party to the Optional Protocol or any other international human rights treaty enabling individual complaints (such as the ECHR) individuals whose rights have been infringed by the NSA are deprived of a direct, effective remedy against the violations they have suffered.

In the case of States which despite best efforts have been unable to identify US surveillance activities and have failed in protecting their subjects, no individual remedy against the violators may be deployed. Those States however, wishing to seek protection and remedies for the individuals under their jurisdiction, may file an international claim against the US for the violation of individual privacy rights, constituting a breach of Article 17 ICCPR. As per Article 41 ICCPR any State party to the convention may address the HRC with a claim against another State party not adhering to the treaty. The US has recognised the HRC competence for inter-State complaints and hence may be targeted with such a claim. Even though the procedure of inter-State complaints has not been exercised so far, primarily for diplomatic reasons, the gravity of the NSA surveillance affair might prove a good occasion for a precedent.[62]

Despite this legal possibility, provided for in Article 41 ICCPR, no State has so far confirmed its plans to address the HRC with a privacy violation claim against the US. States have limited themselves to cutting down on their use of US-based telecommunications services. Brazil led the way with President Dilma Rouseff announcing plans for a "Brazilian Internet", one based on infrastructure and services independent from the US.[63] Seeking ways to free the international network from its

---

[61] For more on the due diligence principle in international law, see generally: Kulesza, J., *Due diligence in International Law*, Brill, Leiden, 2015 (forthcoming).

[62] Such a recommendation was included in the statement of Martin Scheinin in his opinion for the European Parliament on the NSA surveillance scheme. See, Scheinin, LIBE Committee Inquiry statement, *supra* nt. 40.

[63] See e.g., The Independent, Charlton, J., *Brazil plans national Internet redesign in order to avoid US web surveillance*, 18 September 2013, available online at <independent.co.uk/news/world/americas/brazil-plans-national-internet-redesign-in-order-to-avoid-us-web-surveillance-8823515.html> (accessed 24 September 2014); The Guardian, Holpuch, A., *Brazil's controversial plan to extricate the internet from US control*, 20 September 2013, available online at <theguardian.com/world/2013/sep/20/brazil-dilma-rousseff-internet-us-control> (accessed 24 September 2014).

strong technical and economic US dependency, President Rouseff invited national diplomats, international business and community activists from all over the world to a first ever NetMundial—an event offering a unique, multistakeholder platform for Internet governance discussions, with its inaugural meeting focused on plans to limit US dominance of the network. NetMundial was viewed as providing strong support for the UN-led Internet Governance Forum, whose political impact has so far been only limited. The PRISM affair enhanced governmental interest in Internet governance, motivating State authorities to increase their involvement in seeking effective ways for multistakeholder decision making.[64] Other States have also taken steps to limit their US dependency, with, for example, the EU States proposing an EU cloud for storing data of EU citizens according to local privacy laws.[65] Also the recent EU data protection reform has a strong international angle, with Chapter V of the proposed Regulation devoted entirely to protecting EU personal data stored or processed outside the Union.[66] Russia recently adopted laws requiring personal data collected by Internet companies operating in that country to be kept on local servers.[67] Surprisingly, both the EU and Russia might be considered to be following the so-far much criticised Chinese example—it is the Great Firewall of China combined with heavily State-funded local infrastructure that allows China for considerable independence from the US in its Internet-based services.[68] Ironically, the BRIC nations,[69] thus far strongly criticised for their drive towards an internationally controlled and US-independent Internet, seem to lead the way in the fight against universal US cyber surveillance.[70]

Summarising the legal claims provided for in international law for privacy violations by foreign authorities, it must be emphasised that States take primarily diplomatic steps to limit the massive US surveillance and mitigate its results. They act less through international law treaties, and more through diplomacy and soft law forums, often resorting to international business practices, rather than international courts, to influence US security and privacy policies.

---

64 On the role of "multistakeholderism" in Internet governance and international law, see Kulesza, J., *International Internet Law*, Routledge, London, 2012, 125-156.

65 See, European Commission, *European Cloud Computing Strategy*, September 2012, available online at <ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy> (accessed 24 September 2014).

66 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, available online at <ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> (accessed 24 September 2014) (GDPR).

67 Deutsche Welle, Maynes, Ch., *Russia tightens Internet screws with 'server law'*, 11 July 2014, available online at <dw.de/russia-tightens-internet-screws-with-server-law/a-17779072> (accessed 24 September 2014).

68 IT World, Patrizio, A., *BRIC Nations Plan Their own "Independent Internet",* 4 October 2013, available online at <itworld.com/internet/377182/bric-nations-plan-their-own-independent-internet> (accessed 24 September 2014).

69 The abbreviation signifies complementing international policies of Brazil, Russia, India, China, and South Africa.

70 IGF Watch news, Malcolm, J., *India's proposal for a UN Committee for Internet-Related Policies (CIRP)*, 29 October 2011, available online at <igfwatch.org/discussion-board/indias-proposal-for-a-un-committee-for-internet-related-policies-cirp> (accessed 24 September 2014)).

VI. EU Personal Data Reform—How Efficient Is the New Regulation?

The PRISM revelations were one of the key catalysts for the EU personal data reform. In Europe, that is in the European Union States as well as the 48 Council of Europe States bound by the ECHR, privacy is protected through laws on gathering, storing and processing personal data. Personal data is to be understood broadly as any information on an identified or identifiable individual. This intentionally flexible definition is to allow for legal protection over forever new categories of data, including not only names, addresses, health or employment information, but also data provided by geolocation services or social media. The basic requirement for gathering, storing or processing personal data is the consent of the person whom the data concerns, the data subject, which is to be explicitly granted to the controller of such data unless a particular legal provision states otherwise. A controller is understood to be the entity which 'alone or jointly with others determines the purposes, conditions and means of the processing of personal data', while a processor means any person or other body which 'processes personal data on behalf of the controller'.[71] As per those definitions, the controller decides on the gathering, storage and use of the data, while the processor simply follows the controller's instructions. The obligations instituted by the personal data protection laws are directed at both categories of entities.[72] Another general rule present in European data protection law since its inception is that no international transfer of personal data outside the EU is permissible unless the third country offers 'an adequate' level of protection. As per EU law, assessing the adequacy of the protection granted by foreign authorities is left to the European Commission and only upon its decision may a transfer to a third country be performed. When the third country provides no adequate protection, EU States are obliged to prevent data transfers to such countries. The US approach to privacy has been a challenge to EU data protection law since the early 1990s. Since the US does not grant privacy protection to foreigners, an individual compromise between Brussels and Washington needed to be reached. Such was the character of the much controversial Safe Harbor arrangement, an international compromise between the European Commission and US Department of Trade.[73] Limited to a basic compromise on the key guarantees present in the Directive,[74] it proved insufficient, as adherence to the Safe Harbor program led by the Department of Trade was voluntary for US companies and US authorities failed to verify whether those

---

[71] GDPR, *supra* nt. 66, Article 4(5).

[72] *Id.*, Article 43.

[73] For more information on the "Safe Harbor" agreement visit official EU website devoted to this cooperation, European Commission, *How will the "safe harbor" arrangement for personal data transfers to the US work?* available online at <ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm> (accessed 1 December 2014).

[74] These guarantees include the following seven principles: 1) notice (requiring individuals to be informed of their data being collected and ways of its use); 2) choice (possibility of an individual to decide against their data being gathered or processed); 3) onward transfer (further transfer of one's data may be executed only when the third party provides for adequate protection); 4) security (requiring the processor to prevent the data from being lost or misused); 5) data integrity (requiring the processor to ensure the data reliability and use according to the purpose declared); 6) access (enabling the data subject to obtain information on the information about them in the disposal of the processor, as well as to have that information corrected or deleted); 7) enforcement (granting the data subject effective remedy against any infringement of the rights named above).

declaring their compliance with the program actually met its objectives. As a consequence European citizens' data was not protected in the US, even though gathered, stored and processed by US companies in bulk.

The popularity of cloud-based services enhanced the threats to European personal data stored and processed by foreign companies outside the EU. Increasingly, less data was stored in Europe, not allowing local authorities to effectively enforce EU and national privacy laws. It was one of the reasons the comprehensive data protection reform was adopted in Europe in 2014. Aiming to make up for the shortcomings of the 1995 designed framework, the European Commission decided to propose a Regulation, which is directly applicable throughout the Union, rather than a Directive (the Data Protection Directive, DPD), which demanded adoption within national legal systems, often leading to their discrepancies.[75] The primary aim of the reform is to secure personal data originating from the European Union on the global market, moving the current heavy reliance on cloud computing services offered by US companies, and storing Europeans' personal data in the US or off-shoring it to Asia or Africa. It was in 2013 that the elaborate European legal framework for personal data protection proved blatantly ineffective when confronted with the cloud computing design and US national security laws. Differing approaches to individual privacy, discussed above in the context of the contradicting opinion of international law scholars on the universal right to privacy, well known before the PRISM revelations, became the bone of contention between Washington and Brussels, leading to a tight political and economic situation. PRISM was a crucial incentive for the adoption of new, enhanced personal data protection laws as set within the GDPR, whose Chapter V is devoted to transfers of personal data to third countries.[76] As already discussed, one of the principles of EU data protection laws is the prohibition of data transfers outside the Union to countries or territories not grating an 'appropriate' level of protection. The GDPR aims to maintain and elaborate this basic standard, however, following a strong political debate its Article 44 on derogations to this rule is not as strict as one might imagine it to be. Article 44 enumerates cases where controllers, processors and their subcontractors are exempted from data protection obligations. Article 44, paragraph 1(d) allows transfers of personal data to a third country when it is 'necessary for important grounds of public interest'. Recital 87 GDPR lists examples of such public interest, including cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, exchanges between services competent for social security matters, and authorities responsible for prevention, investigation, detection and prosecution of criminal offences.[77] Moreover, as per Recital 56, where personal data might lawfully be processed

---

[75] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DPD), available online at <eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (accessed 24 September 2014).

[76] GDPR, *supra* nt. 63, Recital 98, Article 43. According to Recital 98, the authority providing such a one-stop shop should be located where the controller or processor has 'its main establishment'.

[77] European Parliament, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available online at <europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> (accessed 24 September 2014). As per the EP proposed amendment this prerogative is to go to the European Data Protection Board. EP proposed amendment 102 to Article 8.

on grounds of public interest, the data subject should be entitled to object to the processing, while the burden of proof rests on the controller who is to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject. A significant vice of the proposed regulation is therefore the lack of reference to the validity of a foreign court order, requesting EU personal data from a subject within its jurisdiction. The proposed regulation, although claiming to fend against third-party intrusions, lacks reference to, for example, a foreign court order approval issued by a European court or a requirement for the issuance of such an order under an international agreement, which would significantly enhance local supervision over foreign processing of personal data of EU citizens. Obliging the addressee of such an order—an EU operating company—to inform local European authorities of a request for data from a foreign court or a requirement for local authorisation prior to delivering the requested data by such a company would also seem an efficient measure to ensure the protection of European data against third party interference. No such stipulations are to be found in the GDPR however, although they were originally present in the 2011 draft version of the Regulation.[78] The threat of an unjustified foreign inspection is not effectively mitigated by the moderate phrasing in Recital 90 GDPR allowing for international transfers only 'where the conditions of this Regulation' are met.

In effect, the proposed personal data reform in the EU, although incited by the Snowden revelations, fails to provide effective protection against FISAA. With that in mind, reference to other international law mechanisms is needed.

VII. Human Rights Due Diligence

As discussed above, international law offers certain tools to protect individuals against foreign privacy intrusions. As per the ICCPR national authorities are under an obligation to actively seek ways to protect their subjects from human rights violations inflicted by third parties. Within this category, next to foreign governments, also international corporations are to be identified. States are under an obligation to ensure that companies operating within their jurisdiction also refrain from violating the rights of State residents. Such an obligation was confirmed in 2008 by the UN Special Representative John Ruggie, who produced a report on the interrelationship of business and human rights.[79] The report, although controversial, is recognised as legal justification of certain human rights obligations resting directly on private companies. Ruggie's argument on "human rights due diligence" obligations relies on three assessments, derived from contemporary international law jurisprudence and State practice. The Special Rapporteur non-controversially claims that active human rights protection is one of a State's duties, originating from international human rights law—an argument discussed in detail above. This duty obliges authorities to refrain from human rights violations as well as to protect individuals from human rights infringements by third parties. States are therefore under a direct obligation to identify and prosecute human rights violations of the latter. Ruggie's

---

[78] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 29 November 2011, Article 42, available online at <statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf> (accessed 24 September 2014)

[79] UN Human Rights Council, Protect, Respect and Remedy: a Framework for Business and Human Rights, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, 7 April 2008,A/HRC/8/5.

second argument is more controversial in nature suggesting corporate responsibility for human rights violations by binding international business to universal human rights standards. Ultimately the report contains a postulate for victims' greater access to effective legal and financial remedies. In 2011, the Report resulted in a set of Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (PRR Framework), detailing human rights obligations of international business.[80] This document may be used as a reference for identifying and executing certain human rights obligations of international companies, regardless of their place of incorporation, seat or the market they target. Without the need to engage in confusing debate on limits of State jurisdiction of international companies and international private law, the Ruggie principles and the PRR Framework allow identification of which measures need to be taken by international corporations with respect to individual privacy rights of their users.

As per the PRR Framework, it is a State's duty to guide business on respecting human rights by advising on appropriate methods, including 'human rights due diligence',[81] yet the norms of international human rights law may be applied to business directly. Companies must represent a certain "human rights due diligence" when an individual right is under threat created by their activities.[82] The lack of State action preventing businesses from certain actions or allowing for a certain violation is no excuse for a company's infringement. Principle 17 of the PRR Framework defines a human rights impact assessment as 'assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed'[83] and encourages companies to introduce human rights standards for their customers regardless of the legal requirements effective in their jurisdiction. As a matter of fact, forever more companies, seeking to best cater for their clients' needs, such as Google, Facebook, IBM or Intel have introduced internal privacy policies, seeking to ensure their clients' comfort and trust. The PRR Framework offers a human rights standard for international business, regardless of national laws and differing regional perceptions of individual liberties. Together with the rich body of work on privacy by the HRC, it serves as a good basis for setting privacy policy standards and formulating reasonable expectations for companies processing and trading personal data. The growing consumer awareness of the value of their data requires international companies to cater for their customers' needs also on the level of privacy protection. While international law offers certain solutions against States infringing human rights, as discussed above, it is the PRR Framework that allows direct enforcement of these rights against the companies.

VIII. Summary

While a US company denying an NSA request would likely face sanctions just as much as the employees of its Chinese operating branch could face prison for denying police access to data stored on their machines, there is no doubt that any bulk collection of personal information without legal basis and court supervision is against international

---

[80] Human Rights Council, The Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (Guiding Principles), 21 March 2011, A/HRC/17/31.

[81] *Id.*, 12.

[82] *Ibid.*

[83] *Id.*, 21.

law. The options discussed above all aim to limit this undesired state of affairs. Be it an inter-State complaint under the ICCPR, enhanced diplomatic activity, such as the NetMundial or direct consumer pressure on companies betraying clients' trust, the easily-identifiable international privacy standard seems possible to achieve, despite states or private entities claiming no such standard exists. Consequently, denying corporate responsibility for privacy violations deliberately departs from the truth. It is not the legal notion of privacy that proves troublesome in the global information society, it is the political approach and interests that disallow the existing universal standard to be enforced. The PRISM affair proved the existence and universal recognition of such a right and one is left to hope that the rising awareness of telecommunication service users will lead to a significant change in State surveillance policies.

*

Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You

Els De Busser*

Keywords
DATA PROTECTION; INFORMATION EXCHANGE; OPEN SOURCE DATA; RIGHT TO BE FORGOTTEN

Abstract
Various misconceptions exist regarding open source data, what is meant by this term and how these data can legally be used. This contribution focuses on developing a comprehensive definition of the term and highlights the differences with similar – often confusing – concepts. The fact that open source data are publicly available does not mean that they can be used and processed in any way or for any purpose. As far as open sources contain personal data, the general data protection legislation (national as well as EU and Council of Europe legislation) is applicable. Several difficulties however arise, especially when different types of data are mixed.

This can happen in the context of a criminal investigation. The use of personal data for the purpose of prevention, investigation or prosecution of criminal offences is protected by more specific legal provisions to protect the secrecy of the investigation as well as the fundamental rights of the suspect and the victim(s). The fair trial rights of article 6 ECHR should be respected once a criminal charge has been made.

Open source data are vulnerable for abuse by any individual. Additionally, they are widely available and distributable when the internet is used. In several instances open source data have been used for the purpose of vigilantism (individuals taking law enforcement into their own hands). It is important to draw the line between a legal use of open source data, including the use of open source data for the purpose of a criminal investigation and the illegal use of open source data.

This contribution combines the elements of open source data, personal data and criminal investigations. Answers to the following research questions are sought:

- What are open source data?
- How to protect personal data included in open source data?
- How to use open source data in criminal investigations while respecting data protection legislation?

I. Introduction

Various misconceptions exist regarding open source data, what is meant by this term and how these data can legally be used. This contribution focuses on developing a comprehensive definition of the term and highlights the differences with concepts that seem similar and therefore are often confused. The fact that open source data are publicly available does not mean that they can be used and processed in any way or for any

* Head of Section European Criminal Law, Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany. The author would like to thank Tania Boulot, Nora Römling and Kamand Gharun for their assistance and feedback while preparing this paper.

purpose. As far as open sources contain or consist of personal data, general data protection legislation (national as well as European Union and Council of Europe legislation) is applicable. Several difficulties, however, arise related to the nature of the data and their use or processing.

Besides data protection laws, the use of personal data for the purpose of prevention, investigation or prosecution of criminal offences is also protected by more specific legal provisions to protect the secrecy of the investigation as well as the fundamental rights of the suspect and the victim(s). The fair trial rights of Article 6 European Convention of Human Rights should be respected once a criminal charge has been made. This goes for personal data that are open source as well as closed source data. More and more open source data are used by law enforcement and intelligence services, especially where social media is concerned. In 2012 LexisNexis® Risk Solutions surveyed 1,200 United States federal, state, and local law enforcement professionals concluding that four out of five use various social media networks to assist in investigations with Facebook and YouTube ranking among the most used platforms. This use concerned identifying people and locations; discovering criminal activity and locations; and gathering evidence. Of all respondents, 67% reported believing that social media helps solving crime more quickly.[1] Even though this survey was conducted in the United States, it shows the rising importance of social media as an investigative tool for law enforcement.

Open source data are vulnerable for abuse by any individual. Additionally, they are widely available and distributable when the Internet is used. In several instances open source data have been used for the purpose of vigilantism (individuals taking law enforcement into their own hands). It is important to draw the line between a legal use of open source data, including the use of open source data for the purpose of a criminal investigation and the illegal use of open source data. Lastly, since the Court of Justice of the European Union (CJEU) ruled on a landmark case against Google in May 2014, it is equally relevant to discuss here the catchphrase "the right to be forgotten", the fact that it does not exist and what this debate is really about.

Referring to the so-called Miranda rights in the title—the rights that should be read by US law enforcement officers when taking an individual into custody—is not meant to sound harsh or depressing. It is rather intended to create awareness for Internet and social media users indiscriminately, publicly posting personal data identifying themselves or others. The consequences of this recent trend are not always directly perceived, which makes it all the more difficult to control. Besides raising awareness, this contribution focuses on identifying the precise problem(s) rather than offering concrete solutions.

Combining the elements of open source data, personal data and criminal investigations, this paper intends to offer an answer to questions such as what are open source data; how can personal data included in open source data be protected; and how can open source data be used in criminal investigations while respecting data protection legislation? The legal instruments that are used to answer these questions are the relevant legal instruments adopted by the Council of Europe (CoE) and by the European Union (EU). These include the European Convention on Human Rights (ECHR), the Convention on the processing of personal data by automated means (Data Protection

[1] LexisNexis Risk Solutions, *Role of Social Media in Law Enforcement Significant and Growing*, available online at <lexisnexis.com/en-us/about-us/media/press-release.page?id=134262308548118 1#sthash.pbREo4je.dpuf> (accessed 30 July 2014).

Convention),[2] Resolutions 73(22) and 74(29), and Recommendation 87(15). For the EU the most relevant legal instruments include Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC), [3] the Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Framework Decision 2008), and the legislative proposals that are being negotiated at the present time to reform both the Directive[4] and the Framework Decision.[5] Using these legal instruments does not mean that the geographical scope of this paper is limited to the EU. Rather, all Member States of the CoE are bound by the same data protection standards as well as countries that are not Member States of the CoE.

II. Defining Open Source Data

In order to define what open source data are, it is necessary to first explain what they are not. Open source data are not identical to personal data but can contain or consist of personal data. Traditionally, personal and non-personal data are distinguished based on the characteristic of identifying an individual or enable to identify an individual. Personal data enable one to "single out" a person. The fact whether personal data are open source or not is not part of the definition. On the contrary, the definition of personal data includes any information, which can be open source or closed source. Open source data in their turn can be personal or non-personal.

II.1. Personal Data

The concept of personal data is frequently confused with the right to a private life or privacy. Both concepts overlap, but only to a certain extent. They are certainly not identical. Where personal data are those data that identify or enable to identify an individual, the private life of a person consists of personal as well as of non-personal data. As one of the most difficult concepts to explain—not in the least because of its evolvement in line with technological advancements—the best definition is still the traditional definition introduced by Warren and Brandeis in 1890 describing the right to a

---

2 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, ETS No. 108 available online at <conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (accessed 27 September 2014) (CoE Data Protection Convention).

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available online at <eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN> (accessed 1 2014) (Data Protection Directive 95/46/EC).

4 Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 25 January 2012, COM (2012)11 final, available online at <ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> (accessed 16 November 2014).

5 Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25 January 2012, COM (2012), 10, available online at <eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF> (accessed 3 November 2014).

private life as the right to be let alone.[6] Exercising the right to be let alone and not tolerate interference from private or public persons such as the government, involves more than only personal data.[7] One should thus be careful not to confuse both concepts. Nonetheless, in the jurisprudence of the European Court of Human Rights (ECtHR) the right to a private life has been used to include rulings on personal data. After all, a genuine right to data protection is so far only included in the EU Charter on Fundamental Rights and Freedoms, not in the ECHR.

The data protection standards applicable in the EU and the CoE Member States originate from the CoE Data Protection Convention and two preceding Resolutions.[8] In the Convention and in Directive 95/46/EC, personal data are defined as any information relating to an identified or identifiable individual.[9] Public sector information is also covered by this definition.[10] An identifiable person is a physical[11] person who can be easily identified, meaning not by using very sophisticated[12] methods that should be judged considering technological evolutions.[13]

"Any information" refers to any type of information, objective as well as subjective statements concerning objects, events or persons. Opinions, assessments or conclusions about objects or persons establish subjective information. The format in which the information is held or its carrier is not relevant. Information in any structured or

---

6 Often incorrectly quoted as "to be *left* alone". See Warren, S. D. and Brandeis, L. D., "The right to privacy", *Harvard Law Review*, vol. 4, 1890, 193–220. See also Council of Europe, Parliamentary Assembly, *Recommendation 509(1968) on human rights and modern scientific and technological developments*, 1968, available online at <assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta68/EREC509.htm> (accessed 30 July 2014). This Recommendation started the legislative development of data protection rules and guidelines.

7 See also De Busser, E., *Data Protection in EU and US Criminal Cooperation*, Maklu Publishers, Antwerp-Apeldoorn, 2009, 48–52.

8 The Convention's Explanatory Report explained that the terms and definitions generally follow those used in Resolutions (73) 22 and (74) 29. Some modifications and additions have been made in view of recent national legislation and having regard to the special problems called forth by transfrontier data flows.

9 Article 2(a) CoE Data Protection Convention; Article 2(a) Data Protection Directive 95/46/EC.

10 See Article 29 Data Protection Working Party, *Opinion 3/99 on public sector information and the protection of personal data*, WP 20, 3 May 1999, available online at <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp20_en.pdf> (accessed 30 July 2014).

11 In accordance with Article 3, paragraph 2(b) of the Convention, Member States have the opportunity to declare the provisions of the Convention applicable to legal persons. Declarations in that sense have been submitted by Albania, Austria, Italy, Liechtenstein and Switzerland.

12 The focus on 'very sophisticated methods' as is mentioned in the Explanatory Report to the Data Protection Convention can lead to confusion. One might think that the higher the level of sophistication in the method used in order to identify a person, the less likely it is for the personal information that is detected this way to fall within the scope of the Convention. However—and rightfully pointed out by Bygrave—the higher the level of sophistication is, the easier it is for a person to identify an individual and consequently have access to personal data. Bygrave, L.A., *Data protection law. Approaching its rationale, logic and limits*, Kluwer law International, The Hague, 2002, 43–44.

13 Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 1981, available online at <conventions.coe.int/treaty/en/Reports/Html/108.htm> (accessed 30 July 2014). See also the remarks made by the Court in: *Klass and others v. Germany,* App no 5029/71), para. 4, and ECtHR, 16 February 2000, *Amman v. Switzerland,* App no 27798/95), Section 56. See also Concurring Opinion of Judge Pettiti in ECtHR, 2 August 1984, *Malone v. UK,* App no 8691/79.).

unstructured form (numerical, photographical, acoustic or stored in a computer file)[14] is covered by the definition, taking into consideration future technological developments.

The phrase "related to" would logically mean that the information is about a specific person.[15] However, the EU's Article 29 Data Protection Working Party[16] in a 2005 opinion on the application of Directive 95/46/EC on the practice of RFID-tags[17] stated that this phrase 'refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated'.[18] In view of recent discussions on gathering data on people's online surfing behaviour and personalised online advertising, it is significant that also such data can qualify as personal data. Nevertheless, data gathered by RFID tags or surfing behaviour would not be open source data.

In 2007 the Data Protection Working Party divided the meaning of "relating to" in two parts. On the one hand, certain content is required to make information relate to a person, meaning it should provide in the person's identity, his or her characteristics or behaviour. No purpose or consequence on behalf of the handler of the data is necessary. On the other hand, the use that is made of the information is divided into demonstrating either an element of purpose to assess, treat in a different way or influence a person's status or behaviour or an element of result or impact. The latter refers to the impact on a person's rights and interests or the different treatment of a person as a result, independent of the question whether this result was achieved.[19]

Singling out an individual from the general population or a smaller group of persons by the use of information, or even the possibility of distinguishing an individual from a multitude or a category of persons, constitutes the determining factor in personal data. Identifying someone's unique behaviour can already be sufficient, for example by means of the aforementioned RFID-tags.[20] A person can be isolated directly by using identifying elements such as a name, provided that the name is sufficiently distinctive. Whether more identifiers (address, phone number, physical characteristics, employment information, etc.) are needed, depends on the context. The same piece of information can be personal data in one context and not be sufficient as an identifier in a different setting.[21]

Recital 26 of the Directive 95/46/EC preamble includes a reasonable means-test with regard to the means used for identifying a person. The Data Protection Working Party

---

[14] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, available online at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> (accessed 30 July 2014), 7.

[15] *Id.*, 9.

[16] The name "Article 29 Data Protection Working Party" is derived from the Article 29 of Directive 95/46/EC that set up this working party. It publishes opinions on specific issues related to the application of the Directive.

[17] Radio Frequency Identification Technology stands for a microchip storing data on certain behaviour, for example purchasing behaviour, by the person carrying the tag, which is read by the controller of the tag.

[18] Article 29 Data Protection Working Party, *Working Document on data protection issues related to RFID technology*, WP 105, 19 January 2005, 8.

[19] Data Protection Working Party Opinion 4/2007, *supra* nt. 14, 10–11.

[20] Data Protection Working Party Opinion 4/2007, *supra* nt. 14, 13–14; see also above nt. 17.

[21] See CJEU 6 November 2003, *Lindqvist*, C-101/0101, para. 27. In this case the Court decided on data on an Internet page referring to person's names in conjunction with their phone number or information concerning their working conditions and hobbies, to be personal data within the meaning of Directive 95/46/EC.

added the criteria of cost[22] of conducting the identification, the intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, the risk of organisational dysfunctions and technical failures.[23] All means that are likely reasonably used by the handler of the data to identify the person concerned should be considered by the judge deciding upon a case-by-case-basis. The phrase "likely reasonably" causes confusion as to its exact meaning, in particular by joining such element of probability with the element of difficulty.[24] The fact that the handler of the information would be capable of identifying a person does not necessarily mean that he will in fact put this into practice. However, this would not cause the data to lose their quality of personal data.[25]

During the negotiations on the reform of the data protection legal framework in the EU, the concept of singling out was added to the text of the preamble in the amendments made by the European Parliament.[26] This was not a new notion as the Data Protection Working Party already used it in its 2007 opinion on the concept of personal data.[27] Data that can lead to the singling out of a person from a group of persons thus needs to be so specific—depending on the size of the group[28]—that only one individual can be isolated from the rest of the group.

II.2. Open Source Data

Open source data or open data do not have an official definition that is laid down in any legal instrument. Many documents use the term without defining it, yet limited sources have included their own definition.[29] The common characteristic of the definitions lies in the information being publicly available. When data are closed off from the general public, they can clearly not be considered open source data. When a fee is required to obtain the data, can they still be considered open source? And does it include information on social media profiles that are not public but still open to thousands of users? Where do we draw the line?

---

[22] The Article 29 Data Protection Working Party explicitly mentions the costs as a criterion for concluding on the identification (even though it states it is not the only factor). In 1997 the Council of Europe no longer included costs as a reliable criterion due to developments in computer technology. See Council of Europe, Committee of Ministers, *Recommendation No. R(97)5 on the protection of medical data*, 13 February 1997, available online at <wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=564487&SecMode=1&DocId=560582&Usage=2> (accessed 30 July 2014).

[23] Data Protection Working Party Opinion 4/2007, *supra* nt. 14, 15.

[24] Bygrave, L. A., *Data protection law. Approaching its rationale, logic and limits*, Kluwer law International, The Hague, 2002, 44.

[25] *Ibid*.

[26] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), available online at <europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> (accessed 3 November 2014), Amendment 66.

[27] Data Protection Working Party Opinion 4/2007, *supra* nt. 14, 13.

[28] For example when data refers to a dark haired woman in her thirties living in New York, the group of people will be too large to identify this individual. When the data are more specific and refer to a dark haired woman in her thirties living in New York and teaching English literature at University X in Manhattan, New York City, this would single out a specific individual.

[29] See also Eijkman, Q. and Weggemans, D., "Open source intelligence and privacy dilemmas", *Security and Human Rights*, No. 4, 2012, 286-287.

Open source data is not a new concept as such, demonstrated by the references in guidelines and manuals for intelligence services. Nevertheless, the boom of social media and other sources on the Internet have given it a new dimension by flooding the pool of existing open source data. That does not mean that open source data need to be digital. Even if the majority of open source data today will be found in digital form, observations, photographs or paper publications may just as well be open and publicly available data. The CoE Convention on Cybercrime uses the term open source data, but only indirectly refers to it as publicly available data without giving a definition.[30] With due care not to confuse information and intelligence notions, it is still useful to examine the definitions used in the area of (criminal as well as military) intelligence because open source data are also for intelligence services a necessary source, possibly even a starting point.

The United Nations Office on Drugs and Crime (UNODC) describes open source data as information that is publicly available and adds that one of the main difficulties in working with this type of source is evaluation, as information available in the public domain can frequently be biased, inaccurate or sensationalised.[31] This definition is clearly accommodated towards criminal intelligence analysts and is much wider than information containing personal data. In its Open Source Intelligence Handbook, North Atlantic Treaty Organization (NATO) first separates open source intelligence from academic, business or journalistic research by highlighting that ''it represents the application of the proven process of national intelligence to a global diversity of sources, with the intent of producing tailored intelligence for the commander'.[32] The proven process of national intelligence logically refers to the analysing of information for military purposes. Nonetheless, NATO's discerning definitions of four types of information and intelligence are relevant in this discussion due to the elements of restriction of information for a specific person or group of persons on the one hand and the element of verification or accuracy on the other hand. According to NATO, open source information means that a form of processing has taken place from the raw open source data.[33] It refers to those data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. Open source information is thus generic information that is usually widely disseminated and includes newspapers, books, broadcast, and general daily reports. Open source intelligence refers to information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question. This type of information applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence. A more advanced type of information is the validated open source intelligence. This is defined as information to which a very high degree of certainty can be attributed. It can be produced by an all-source intelligence professional, with access to classified intelligence sources. It can also

---

[30] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, ETS No. 185, 8 November 2001, available online at <conventions.coe.int/Treaty/en/Reports/Html/185.htm> (accessed 3 November 2014).

[31] United Nations Office on Drugs and Crime, *Criminal Intelligence - Manual for Analysts*, 2011, available online at <unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf> (accessed 20 July 2014), 12.

[32] NATO, *Open Source Intelligence Handbook*, 2001, available online at <oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf> (accessed 20 July 2014), 1–3.

[33] Open source data is defined as the raw print, broadcast, oral debriefing or other form of information from a primary source.

come from an assured open source to which no question can be raised concerning its validity.[34] Open source data and open source information are thus in the NATO definitions meant for a wider audience and have been subject to a lower degree of scrutiny, while open source intelligence and validated open source intelligence are rather conclusions drawn from the data and information, the degree of accuracy and reliability is higher and it is meant for a restricted audience.

Open source data can be authored and developed by any person. In some cases the author or producer is unknown and the reliability or accuracy cannot possibly be verified, for example fake profiles on social media. In other cases, such as journalism, the author is known and the information has a high degree of reliability and accuracy. Still this is considered open source data.[35] It is thus not relevant for the description of open source data whether its reliability and accuracy has been checked.

The size of the audience to whom the data are available brings up the question of payment. Can data that is only available on payment be considered open source or not? It would not be realistic to limit the definition of open source data to freely available data as technically one would have to consider the cost of Internet connections even when newspapers or social media have freely accessible websites.[36] However, open source data can also exist in the offline world. For example, an expensive book or report can be publicly available, but due to its price, it is limited in accessibility. For this reason the element of payment should not be included in the definition of open source data, rather the aspect of availability to a wide or restricted public is significant. A restricted public is not the general population but a group of people that is separated from the general population based on one or more filtering conditions such as their professional occupation, their paid or unpaid subscription to a newspaper or their friendship with a person on a social media profile. The latter brings up a particular question regarding the threshold that is required. When the account holder of a Facebook profile that is not public posts information, one would tend to label this information as closed source data. However, if this Facebook user has over 5,000 friends, can we still rightfully speak of closed source data? In addition, every one of these friends can share the information with his or her friends creating a snowball effect and an uncontainable distribution of the information. The same goes for a newspaper that has thousands of paying subscribers who can spread information further. A solution could be to interpret the term "restricted public" as referring to the ability to specify the recipients of the data and to limit the dissemination of the information. This interpretation results in any information that is posted on a Facebook profile allowing the friends of the account holder to share, should be labelled as open source data. This does not mean that any person can do anything he or she wants with the data, for two reasons. First, the fact that such data are open source does not mean that they are reliable or accurate. Second, open source data can contain personal data. If this is the case they are protected by data protection regulations.

Developing a definition of open source data that is not exclusively meant for the field of criminal and military intelligence, it is clearer to describe what open source data are not rather than to describe what is covered by the term. Based on the analysis above,

---

[34] Explanatory Report to the Convention on Cybercrime, *supra* nt. 30.

[35] See above, nt. 29.

[36] Even in the description of personal data in 1997, the Council of Europe did not consider cost a reliable criterion due to the developments in computer technology. Council of Europe Committee of Ministers, *Recommendation No. R(97)5 on the protection of medical data*, 13 February 1997, available online at <wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=564487&SecMode=1&DocId=560582&Usage=2> (accessed 30 July 2014).

open source data can be described as any information that is not restricted to a specified public and that is not necessarily reliable or accurate. Whether or not the information identifies or enables to identify an individual is not part of the definition since open source data can include both personal data and non-personal data.

III. Personal Data Protection

When open source data contain personal data, they are protected by the traditional data protection standards. These are laid down in binding legal instruments. The data protection legal instrument that has the widest geographical scope and is also the oldest international convention on this matter is the 1981 CoE Data Protection Convention. Ratified by forty six states, the Convention has introduced the basic principles to be complied with when personal data are processed. Even though its scope is limited to automatic processing, many states have widened the scope of their implementing legislation to also include non-automatic data processing. In this part, the data protection standards are applied to the central theme of open source data including the particular challenges that this type of data can raise for data protection.

III.1. Data Protection Standards

As the basic binding[37] legal instrument, the Data Protection Convention sets out the five minimum requirements personal data should fulfil. Article 5 of the Convention was based on the text of two older CoE Resolutions[38] and distinguishes two groups of standards: quality standards for personal data on the one hand, and quality standards for the processing of personal data on the other hand. Both are divided into more detailed principles that will be dealt with here in line with the two fundamental legal standards presented by the CoE.[39] Besides the data subject giving his or her consent, derogations are allowed but only in accordance with Article 9 that is in turn based on the provisions of Article 8 ECHR. It should be pointed out that for the EU Member States, the standards of the Convention have been implemented and further specified in Directive 95/46/EC for commercial matters and in Framework Decision 2008 for criminal matters.

---

[37] As non-binding instruments, the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, C(80)58/Final, 23 September 1980 (OECD Guidelines) and the United Nations Guidelines concerning Computerized Personal Data Files, General Assembly, 14 December 1990, encompass the same basic principles, leaving room for national legislators to implement data protection rules based on these guidelines (UN Guidelines).

[38] Resolution (73) 22 of the Committee of Ministers of 26 September 1973 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, available online at <wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2> (accessed 21 September 2014); Resolution (74)29 of the Committee of Ministers of 20 September 1974 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Public Sector, available online at <wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2> (accessed 21 September 2014). .

[39] Explanatory Report of the Council of Europe Convention for the Protection of Individuals with Regards to the Automatic Processing of Personal Data, ETS no. 108, Section 40, available online at <conventions.coe.int/Treaty/EN/Reports/Html/108.htm> (accessed 27 September 2014).

III.1.1. Quality Standards for Personal Data

III.1.1.1. Accuracy and Reliability

Ensuring the accuracy of personal data that are processed and updating them whenever necessary is the first standard of data protection. In other words, this standard assures the correspondence of the data to the reality they refer to, such as a person's name and address, employment status, health data, etc. The Data Protection Convention provides the data subject (the person who is identified by the data) with the right to have data corrected or erased if they do not comply with this standard. This implies notification to the data subject of the fact data were gathered and the purpose thereof, unless the individual already has this information or unless other exceptions apply such as the prevailing interests of an ongoing investigation.

As additional protection, Directive 95/46/EC assigns the data controller as the responsible party for ensuring the accuracy of the data as well as updates.[40] The data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.[41] The frequency of updates is not regulated. Although United Nations (UN) Guidelines recommend updates to be held regularly or when the data contained in a file are used,[42] the Convention and the Directive limit updating data to "where necessary".[43] The Organisation for Economic Co-operation and Development Guidelines mention that data quality standards are not intended to be more far-reaching than is necessary for the purposes for which the data are used.[44] For example, data processed for historical or statistical purposes do not necessarily need updating.

In accordance with the definition of open source data developed in this contribution, they are not necessarily accurate or reliable. When open source data contain data that identify or enable to identify an individual however, they should also be updated or corrected when necessary. Considering the possibly wide and uncontainable distribution of open source data, updating and correcting can only be done at the source, whether this is an update on a social media page or a newspaper publishing an erratum. Logically, the data subject can enforce his or her right to correct or erase false personal data that are open source.

---

[40] Article 6, Section 1(d) and Section 2, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available online at <eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (accessed 27 September 2014).

[41] *Id.*, Article 2(d).

[42] Article A.2, GA Resolution 45/95 (68th plenary meeting) A/RES/45/95 14, December 1990.

[43] Article 5(d) CoE Data Protection Convention; Article 6(1)(d) Data Protection Directive 95/46/EC.

[44] Article 53, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available online at <oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> (accessed 27 September 2014).

III.1.1.2. Adequate, Relevant and Proportionate Personal Data

Personal data should be adequate, relevant and not excessive in relation to the purposes they are gathered and processed for. The Data Protection Convention[45] and the Directive[46] provide for a qualitative and a quantitative condition;[47] no personal data should be collected and stored in view of a potential future use, without having an exact view on the purpose it would be used for.[48] This was one of the reasons why on 8 April 2014 the CJEU annulled the controversial Directive 2006/24/EC (Data Retention Directive) obliging telecommunication providers to store personal data for periods of time up to two years in case they may be needed in a future criminal investigation or prosecution.[49]

A qualitative connection should exist between the personal data and the purpose. If there is no direct nexus—for example the same result can be achieved by other less intrusive means[50]—the data are not adequate or relevant in relation to the purpose. No personal data can be processed for undefined purposes,[51] a specified purpose should be provided as well as a direct link between purpose and data. Respecting the proportionality rule means that the data controller should determine and distinguish the minimum amount of personal data needed in order to successfully accomplish a specific purpose and limit its processing to these data.[52] Blanket data collection or fishing expeditions[53] are not in line with the data protection standards.[54]

The purpose for the processing of personal data included in open source data could be journalistic purposes or academic research. Determining whether personal data are in such cases adequate, relevant and not excessive can be challenging. The recent case before the Court of Justice on the debated and often misunderstood catchphrase 'the right to be forgotten' demonstrates how difficult the adequacy and relevance of personal data in open source situations can be. For this reason a separate part of this contribution is dedicated to an analysis of the Court of Justice ruling of spring 2014.

---

45 Article 5(c), CoE Data Protection Convention.

46 Article 6, Section 1(c), Data Protection Directive 95/46/EC.

47 Also the non-binding UN Guidelines, Section A.3 and OECD Guidelines, para. 53 provide in this rule.

48 This should be distinguished from the case in which data are gathered and kept for a particular foreseeable emergency which may never occur, for example, where an employer holds details of blood groups of employees engaged in hazardous occupations. Information Commissioner, Data Protection Act 1998, Legal Guidance, 1998, 37.

49 European Court of Justice (ECJ), 13 May 2014, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12.

50 For example the Belgian Privacy Commission did not authorise the National Organization for the Identification and Registration of Dogs access to the national register of inhabitants based on the lack of proportionality, since in case a dog owner should be contacted, local or federal police authorities can be involved in order to find the owner's contact data. Belgian Privacy Commission, Advise no. 38/2001, 8 October 2001.

51 *Open Source Intelligence Handbook, supra* nt. 32, 41.

52 Information Commissioner, Data Protection Act 1998, Legal Guidance, 1998, 36.

53 Fishing expeditions refer to random and untargeted searches in a large collection of data in an attempt to find relevant information.

54 See Committee of Ministers, Resolution (1973) 22, Article 21, in which adopting a rule that would 'halt unbridled hoarding of data' is recommended.

III.1.1.3. No Such Thing as a Right to Be Forgotten

The so-called right to be forgotten became a catchphrase in 2012 with the launch of the EU data protection legal framework reform. The term however is fundamentally incorrect. There is no such thing as a right to be forgotten and there never will be as long as the individual human memory and the collective memory cannot be physically tampered with.[55] What exists in accordance with applicable data protection rules is a right to have personal data corrected, updated or deleted when necessary. This is nothing new as this right has been in existence since the aforementioned data quality standards were laid down in the 1981 Data Protection Convention.

On 13 May 2014 the Court of Justice ruled on a preliminary question brought before it by the Spanish Audiencia Nacional. The Court decided that the world's most popular search engine Google is responsible for removing links to personal data that are no longer relevant to the purpose they were processed for. Data subject in the case is Costeja González, a Spanish citizen who had social security debts in the late nineties. The recovery of these debts led to a real-estate auction that was in accordance with an order by the Ministry of Labour and Social Affairs announced in newspaper La Vanguardia with the purpose to give the auction maximum publicity and attract as many bidders as possible. In 1998, not every newspaper had an online version as is the case today. Also, La Vanguardia has in the meantime made its publication and archive available online, including the announcement mentioning Costeja González. When he realised the open source availability of this information after a Google search on his name, he submitted complaints with the Spanish data protection authority against the newspaper and against Google. According to the data protection authority, the publication by La Vanguardia was legally justified because of the order by the Ministry of Labour and Social Affairs. As a result, this complaint was rejected. The complaint against Google and the request that Google remove the links to the published personal data was brought before a national judge, who sent a request for a preliminary ruling to the Court of Justice. Contrary to what the Advocate General to the Court of Justice concluded, the Court first of all considered Google a data controller for the activity consisting in finding information published or placed on the Internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to Internet users according to a particular order of preference. Secondly, the Court considered the search engine also responsible for removing the links making the information concerning Costeja González available on the Internet.

The personal data as such are not contested in this case as they are not incorrect. Nevertheless, according to Costeja González an announcement for a real-estate auction held in 1998, published for the purpose of ensuring a higher amount of bidders has lost all relevance two decades later. Because personal data should be relevant for the purpose they were processed for, and should not be stored in a database longer than is necessary for that purpose, thus far the Court of Justice's ruling is acceptable. Holding Google responsible for the fact that this announcement is still available today however is focusing on the wrong target. Google only makes information that already exists searchable and creates an index of search results; it did not create the data, nor was Google the source of the information as such. Requiring Google to remove the links is not the correct issue to

[55] See also De Hert, P. and Papakonstantinou, V., "How the European Google Decision May Have Nothing To Do With a Right to Be Forgotten", *Privacy Perspectives*, International Association of Privacy Professionals, 19 June 2014, available online at <privacyassociation.org/news/a/how-the-european-google-decision-may-have-nothing-to-do-with-a-right-to-be> (accessed 27 September 2014).

address from a data protection point of view. Even after removal of the link, the information is still available on the La Vanguardia website. Many countries have legal provisions on the publication of certain announcements or judgments that entered into force before the development of the Internet. In the meantime, the concept of publication has evolved. It now also includes online publication, making newspapers available on a wider scale and for a possibly indefinite period of time. The real issue here is the fact that the personal data are still present on the La Vanguardia website two decades after it was legal and necessary to publish it for a particular real-estate auction. The correct target is therefore the national Spanish law and its data retention provisions, not Google. The Court of Justice was logically limited by the scope of the request for a preliminary ruling but could have at least ruled that Google was not responsible for removing the links in question.

Besides the described data protection issue in this case, it is also dangerous to put a private company in a position to decide whether or not the link to certain information is relevant. A search engine's interests are of a commercial nature and do not encompass the rights of the data subject. This is a task for a data protection authority or a judge, not a private company. Moreover, Google is now overwhelmed with over 90,000 requests for the removal of links since the Court of Justice ruling.[56] The company has even reinstalled links to newspaper articles from the Guardian after the British newspaper protested their removal.[57] This shows the difficulties for a private company to be in such a position and the inevitable tension with the freedom of information.

III.1.2. Quality Standards for the Processing of Personal Data

Personal data should be obtained and processed fairly and lawfully. This data protection rule means that gathering personal data, and as a possible result infringing upon a person's right to a private life, can only be done when this encompasses lawfully derogating from Article 8 ECHR. In other words, the gathering of personal data must be laid down in law, it should have a legitimate aim and it should be necessary in the interest of protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences or in the interests of protecting the data subject or the rights and freedoms of others. Two principles complete the quality standards for data processing: the purpose limitation principle and the data retention principle.

---

[56] Schechner, S., "Google Grants Majority of 'Right to Be Forgotten' Requests", *The Wall Street Journal*, 24 July 2014, available online at <online.wsj.com/Articles/google-grants-more-than-half-of-right-to-be-forgotten-requests-processed-so-far-1406223241?mod=yahoo_hs> (accessed 27 September 2014).

[57] Lee, D., "Google reinstates 'forgotten' links after pressure", *BBC News*, 4 July 2014, available online at <bbc.com/news/technology-28157607> (accessed 27 September 2014).

III.1.2.1. Purpose Limitation

In the aforementioned 1973 Resolution of the CoE, purpose limitation first made its introduction when the need was felt to control the use made of information stored in electronic databanks.[58] The purpose limitation principle means that personal data should be stored for specified and legitimate purposes only and should not be used in a way that is incompatible with those purposes. In other words, the purpose for which personal data may be processed is either the original purpose they were collected for or a purpose that is compatible therewith. What exactly constitutes a compatible purpose is not defined by the Data Protection Convention or its explanatory report. It was not until 2013 that the EU Data Protection Working Party published an opinion on what should be understood by the term "compatible purpose".[59] Rather than offering a strict definition of compatibility, which would be too stringent, the Working Party listed key indicators to be considered when assessing compatibility. These are the relationship between the purposes for which the data have been collected and the purposes of further processing, the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use, the nature of the data and the impact of the further processing on the data subjects and the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects. Since this is an opinion, it is not legally binding. Nevertheless, it offers guidance to data controllers, data protection authorities or judges deciding on the matter.

In this respect, Article 8, paragraph 2 ECHR should be referred to, since every interference with the right to privacy should be legal and necessary in the interests of a legitimate aim. Even with the difference between the right to privacy and the processing of personal data described above, derogating from both is governed by the same restrictions as Article 9 of the Data Protection Convention is modelled on the provisions of Article 8, paragraph 2 ECHR. Lawfully derogating from the data protection standards will be discussed in the next sub-section of this paper.

III.1.2.2. Purpose Limitation and Open Source Data

The significance of purpose limitation for open source data lies in the fact that the public availability of open source data raises the risk of processing for incompatible purposes. Any personal data that can be drawn from an open source, such as statements or pictures, posted on a public social media profile can be misused for other purposes.[60]

---

[58] Committee of Ministers, Resolution (73)22 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Private Sector, 26 September 1973. In addition a similar Resolution was adopted on the protection of privacy of individuals *vis-à-vis* electronic data banks in the public sector, Committee of Ministers, Resolution (74)29 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Public Sector, 20 September 1974. The Explanatory Report to Resolution (73)22 demonstrates the fear of data abuse: 'There is a certain risk that the user of a data bank, in order to pay off the cost of storing data, might try to find new applications for which the data in his possession could be used. If such applications were to go beyond the original purposes for which the information had been compiled, a violation of the right of the persons concerned to privacy might ensue.'

[59] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, 23–27, available online at <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (accessed 27 September 2014).

[60] This does not mean that a data protection infringement is the only possibly intrusion, (criminal) offences such as defamation and slander could occur or intellectual property rights could be disrespected. These, however, reach outside the scope of this contribution.

The first question is what the original purpose of the open source data is. In some cases such as academic research or journalism this can be clear, in the case of social media the purpose for publishing personal data can range from holiday pictures to wedding announcements, informing people of a new phone number or simply chatting. The bottom line is communication. Perhaps one could even consider social media as a purpose in itself combining the communication element with the element of spreading information on oneself to a limited group of persons or to the general public.[61] An example of misusing open source data could be the public posting of a birth announcement—including the address of the new parents—on a social media page that is followed by an insurance company sending the parents folders for life insurance.

This seems similar to behavioural advertising but the difference is that the latter uses cookies or similar devices installing software on Internet users' computers to track their surfing behaviour, enabling them to show users personalised ads on specific webpages. The EU Data Protection Working Party has argued that the use of such identifiers enabling the creation of very detailed user profiles can in most cases be considered personal data processing, so users' prior consent for installing cookies is required.[62] This does not concern open source data since the surfing behaviour can only be tracked by specific software that is connected to companies' websites; thus the data that are gathered are restricted to a specified public.

When personal data on social media are publicly available, often the perception is that these may be used for any other purpose by anyone. Nonetheless, traditional data protection laws still apply and besides the described compatible purposes, such personal data, may only be used when the legality and necessity requirements are fulfilled. A typical example is a criminal investigation. The riots in several London neighbourhoods in 2011 led not only to the arrests of those inciting the looters on Facebook and Twitter, but also those who had unwisely posted pictures of themselves on social media with stolen goods. In the next part of this contribution, the use of open source data for criminal investigations and prosecutions will be discussed further.

III.1.2.3. Retention of Personal Data

Even if personal data are adequate, relevant and not excessive at the moment of their collection, after a certain amount of time these data could be no longer adequate and relevant in relation to the purpose they were gathered for. This was the case in the recent ruling by the Court of Justice against Google (see above).

The longer personal data are stored for, the higher the risk of intentional or unintentional misuse becomes.[63] The data retention principle specifies that personal data can be saved in databases for as long as is required for the purpose they are stored for. After this period of time has passed, the data can still be retained but need to be separated from the identifying factor, removing the quality of personal data. This separation does not need to be permanent, it is sufficient that the identification of the person concerned cannot be done easily.[64]

---

[61] Oxford Dictionary defines social media as websites and applications that enable users to create and share content or to participate in social networking.

[62] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, 9, available online at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf>.

[63] Committee of Ministers, Resolution (73)22 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Private Sector, 26 September 1973, paras. 23–25.

[64] *Open Source Intelligence Handbook, supra* nt. 32, 42.

Derogating from the data retention principle is lawful under the same conditions as explained above. In other words, personal data can be stored for longer than necessary, but this must be laid down in law and it needs to be necessary in the interests of protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences or in the interest of protecting the data subject or the rights and freedoms of others. Before declaring the Data Retention Directive invalid, the Court of Justice confirmed that the fight against serious crime is indeed of the utmost importance in order to ensure public security. However, according to the Court such an objective of general interest cannot in itself justify a retention measure such as that established by the contested Directive being considered to be necessary for the purpose of that fight. In addition, the Court criticised the text of the Directive since it covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. The Directive applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a direct or remote link with serious crime. It does not provide for any exception, meaning that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy. Therefore, the Directive does not limit the processing of personal data to what is strictly necessary.[65]

III.1.2.4. Data Retention and Open Source Data

A significant issue with open source data and data retention is the lack of control. The availability of the data gives them a perceived outlaw-status. Without the data subject's knowledge, data identifying him or her can be copied and stored on servers, computers or portable devices where they may remain stored for very long periods of time and may or may not impact the data subject's life at a much later stage, as was the case in the aforementioned judgment against Google. Similar issues rise with public pictures or statements on social media that can be easily found online by potential employers negatively influencing their image of the data subject. For the reasons set out above, search engine operators should not be made responsible for providing links to open source data that are online.

In case a data subject would want to file a complaint against such retention and misuse of personal data, it is thus not the search engine but the website keeping the personal data in their databases that should be the target.

III.2. Derogating from Data Protection Standards

The lawful ways of derogating from the data protection standards have been briefly touched upon above. Not being able to derogate from these standards would hinder many forms of data processing that have legitimate aims and are necessary for the functioning of a democratic society, such as the prevention, investigation and prosecution of criminal offences. When open source data that contain or consist of personal data are processed outside the scope of the data protection standards, the processing should fulfil the requirements of legality and necessity.

Typically it is the necessity requirement that causes most difficulties in practice. The requirement of necessity was introduced in order not to give a state too much leeway and to identify a pressing social need. Still it encompasses a range of interests—fundamental

---

[65] ECJ, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C 293/12 and C 594/12, 51–58.

values in a democratic society—that could make derogating from the standards necessary.[66] The protection of state security refers to internal and external threats, making it legal to violate privacy rights—for example by conducting a telephone tap—in the context of an investigation against an attack on state institutions but also the gathering of intelligence. This derogation could therefore be used for allowing the use made of personal data by security services provided there is a nexus with a specific investigation. The monetary interests of the state refer to tax collection requirements and exchange control.[67] It does not entirely cover the economic well-being of the state, which was the wording used in Article 8, paragraph 2 ECHR. It covers however a specific part of it, namely all means of financing a state's policies. It is important—especially for the next part of this contribution—which the suppression of criminal offences does not require a criminal charge has been made against the individual involved. Where Article 8, paragraph 2 ECHR provides an exception for the prevention of disorder or crime, it encompasses a wider range of acts than merely investigation and prosecution of a criminal offence.

In its jurisprudence the European Court of Human Rights (ECtHR) has added three conditions: infringements of the right to a private life should also be precise, foreseeable and proportionate.[68] This means that every time an individual's right to a private life is restricted, the restriction should be counterbalanced by the assurance that it is legal and necessary for fulfilling a legitimate aim. Besides the fact that the legal provisions describing the allowed infringement should be precise enough, the individual should be able to predict from the relevant law in which cases his or her personal data could be collected and processed and these provisions should be precise and foreseeable in order for the individual to regulate his or her conduct accordingly.

Derogating from the right to a private life by processing personal data needs to be proportionate to the legitimate aim that is pursued. Proportionality is thus a requirement for the data itself as well as for the processing of the data. On the one hand, the personal data gathered by means of infringing upon an individual's privacy should not be excessive in quantity in relation to the objective to be served, for example the annulment of the Data Retention Directive was besides the potential use also based on the massive and undiscriminating retention of data. On the other hand, regardless the amount of data gathered, in cases where the same result could have been accomplished with actions that are less privacy-intrusive the proportionality requirement is not fulfilled.

The foreseeability aspect relates to the clarity of the legal provisions on processing of personal data as exceptions to the right to a private life. National data protection laws should be sufficiently clear in defining what constitutes a compatible purpose due to the interference with an individual's private life that the use of personal data entails. It is, however, not enough to simply provide in sufficiently clear laws. The EU Data Protection Working Party stated that in practice, laws should not only mention the final objectives of the legislative measure and designate the controller of the processing. They should also specifically describe the objectives of the relevant data processing, the

---

66 CoE Data Protection Convention, *supra* nt. 2, paras. 55–56.

67 *Id.*, para. 57.

68 European Data Protection Supervisor, Third Opinion 27 April 2007 on the Proposal for a Council Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Cooperation in Criminal Matters, *O.J.* C139, 23 June 2007, 5, available online at <secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-04-27_3dpillar_3_EN.pdf> (accessed 27 September 2014); ECtHR, 2 August 1984, *Malone v. UK*, 8691/79, paras. 67–68; and ECtHR, 4 May 2000, *Rotaru v. Romania*, 28341/95, para. 55.

categories of personal data to be processed, the specific purposes and means of processing, the categories of persons authorised to process the data, the procedure to be followed for the processing, and the safeguards against any arbitrary interference by public authorities.[69]

Derogating from the rule of purpose limitation or from the data retention principle can only be foreseeable if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his or her conduct. The individual should be able to predict the consequences of certain behaviour to a reasonable degree. However, the consequences should not be foreseeable with absolute certainty.[70] This requirement implies a responsibility on behalf of a state's legislator to design clear-cut and transparent provisions when enacting measures that interfere with individuals' right to a private life. In the judgment annulling the Data Retention Directive the Court of Justice criticised the EU legislator for not limiting data retention to what is strictly necessary. On EU level objective criteria should have been formulated, according to which the national legislators could limit the periods of data retention as well as the access rights to the databases.

IV. Evidence in Criminal Investigations

Open source data can and will be often used as evidence in criminal investigations. Based on their impact on the human rights of the individual(s) concerned—suspect, victims, witnesses, etc.—and on the society or community in which a criminal offence has been committed, criminal investigations and prosecutions are regulated by a special set of rights. The information that is used to investigate the offence and to establish the truth will also contain personal data, whose processing is regulated by the data protection standards discussed above. Open source data can equally be included in criminal investigations and prosecutions, triggering separate issues. In this section, these issues are identified after introducing the correct terminology and the rights to be considered.

IV.1. Information, Intelligence and Evidence

Before engaging in a discussion on investigations into criminal offences and the evidence used in criminal proceedings, it is important to understand the difference between the terms "information", "intelligence" and "evidence". Similar to NATO's explanation (see above), the UNODC explained the relevant terminology and stated that information is raw data of any type, whilst intelligence is data that has been worked on, given added value or significance. Information is evaluated through a process of considering it with regard to its context through its source and reliability.[71] This could, for example, include the combining of information with other information, the "connecting the dots" process.

Obviously information can consist of open source data. By interpreting open source data and giving them meaning, intelligence can be obtained. This is not yet evidence. Evidence is information and intelligence that is used to establish proof of one of more criminal offences. Which evidence is admissible and how evidence can be presented is

---

[69] See above nt. 22, 38.

[70] ECtHR, 16 February 2000, *Amman v. Switzerland*, 27798/95, para. 56; ECtHR, 26 April 1979, *The Sunday Times v. United Kingdom*, 6538/74, para. 49.

[71] United Nations Office on Drugs and Crime, *Criminal Intelligence – Manual for Analysts*, 2011, 1-2, available online at <unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf> (accessed 20 July 2014).

regulated by national laws. In principle there is no objection for open source data not to become evidence in criminal proceedings when they are relevant for the case and they are admissible as evidence. However, when open source data consist of personal data, then data protection standards should be complied with. Stating that police can use the information on a public social network profile without any restriction is thus incorrect.[72]

Besides the described data protection standards, another set of rights should be respected once a criminal charge is made: the so-called fair trial rights of Article 6 ECHR. In this context it is relevant to highlight the relationship between Article 6 and Article 8 ECHR. The latter describes the right to a private life, which is not identical to the right to data protection. At the present time only the EU has adopted a genuine right to data protection, in the Charter on Fundamental Rights and Freedoms. In the jurisprudence of the ECtHR however, the right to private life has been used to protect personal data as well. Therefore it is relevant to include the tension between Article 6 and Article 8 ECHR in this discussion.

IV.2. Fair Trial Rights

Article 6 ECHR is often referred to as the fair trial right, since it encompasses inter alia the requirement of an independent and impartial tribunal; the presumption of innocence and the right to a confrontation of witnesses. These rights should protect the defendant from arbitrariness or prejudgment in the course of the proceedings. Article 6 is applicable in civil as well as in criminal proceedings. However, when criminal proceedings are concerned, it is only applicable after a criminal charge has been made. In *Deweer v. Belgium*, the ECtHR determined this moment by means of the official notification of the allegation that the individual concerned has committed a criminal offence or an implication thereof has been given.[73] Whether or not a charge was criminal—and not administrative—was interpreted in further case-law. For a criminal charge it is necessary that the relevant national provisions belong to the criminal law of a state, disciplinary law or both, and when the nature of the offence and the severity of the penalty are considered to be criminal.[74]

Gathering information and intelligence is for a large part done before a criminal charge is made; usually it is needed in order to make a criminal charge. This would mean that the evidence derived from this information and intelligence would fall outside the scope of Article 6. With regard to the proactive use of special investigative techniques to collect information, the CoE has adopted specific recommendations. [75] Special

---

[72] Voigt, S., Jansen, N. and Hinz, O., "Law Enforcement 2.0 – The Potential and the (Legal) Restrictions of Facebook Data for Police Tracing and Investigation", *European Conference on Information Systems 2013 Completed Research,* 2013, available online at <staff.science.uu.nl/~Vlaan107/ecis/files/ECIS2013-0141-paper.pdf> (accessed on 25 July 2014).

[73] ECtHR, 27 February 1980, *Deweer v. Belgium*, 6903/75, para. 46.

[74] ECtHR, 8 June 1976, *Engel and others v. the Netherlands*, 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, para. 82; ECtHR, 21 February 1984, *Öztürk v. Germany*, 8544/79, paras. 55–56.

[75] Council of Europe, *Guidelines on Human Rights and the Fight against Terrorism*, 11 July 2002, available online at <umn.edu/humanrts/instree/HR%20and%20the%20fight%20against%20terrorism.pdf> (accessed 1 October 2014); Council of Europe, *Recommendation Rec(2005)9 to member states on the protection of witnesses and collaborators of justice*, 20 April 2005, available online at <wcd.coe.int/ViewDoc.jsp?id=849237&Site=COE> (accessed 1 October 2014); Council of Europe, Recommendation Rec(2005)10 to Member States on special investigation techniques in relation to serious crimes including acts of terrorism, 20 April 2005, available online at <wcd.coe.int/ViewDoc.jsp?id=849269> (accessed 1 October 2014).

investigative techniques will not be needed when open source data are concerned. The question remains whether open source data that consist of personal data and have been collected before a criminal charge was made, can be used as evidence in criminal proceedings.

IV.3. Gap between Article 6 and Article 8 ECHR

Article 8 ECHR prohibits unnecessary interference with an individual's private life. It can be derogated from, provided that this is laid down in clear-cut and accessible legislation and provided it is necessary in the interests of preventing disorder or crime. Accurate information should be provided to the competent authorities that violation of a person's right to a private life is in fact genuinely preventing disorder or crime.[76] When it is clear to public authorities that there is little or no risk of disorder or crime occurring, they should refrain from interfering in a person's private life.[77]

Even though it was pointed out before that in the ECtHR jurisprudence Article 8 ECHR is used to protect personal data, it can still only serve as a basic rule and not as a detailed set of provisions for protecting personal data that are gathered for the purpose of prevention, investigation, prosecution and punishment of criminal offences. Article 6 ECHR in its turn protects the individual against whom a criminal charge was made but does not foresee in specific rights protecting the individual's private life or personal data.

The ECtHR has ruled more than once on the effect of a violation of Article 8 on the trial. In *Schenk v. Switzerland* and *Teixeira de Castro v. Portugal*, the Court considered it not necessary to discuss Article 8 after deciding on Article 6. In the first case no breach of Article 6 was detected due to the disputed recording of a private telephone conversation not being the only evidence.[78] In the Teixeira de Castro case the use of evidence as a result of incitement by undercover agents meant a clear breach of the right to a fair trial, so the Court did not see a need to consider the complaint on a breach of Article 8 separately.[79] In the Khan case, however, the Court took a stand on the relationship between Article 6 and Article 8. It ruled that a fair trial had been provided to the applicant who received due opportunities for challenging the evidence, even after confirming a breach of Article 8 based on the use of unlawfully installed listening devices.[80] With this judgment the Court cut the link between Article 6 and 8. The ruling is inspired by the established ECtHR case law stating that the right to a fair trial is based on all circumstances of the case. The proceedings as a whole, including appeal and cassation, should be part of the assessment whether a fair trial has taken place or not.[81] Rules on the admissibility of evidence as such are not within the ECtHR's competence. However, the Court concluded that, as long as the defendant has been given the

---

[76] ECtHR, 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, 62332/00, paras. 89 and 92. See also ECtHR, 6 September 1978, *Klass and others v. Germany*, 5029/71, para. 48; ECtHR, 25 December 2011, *P.G. and J.H. v. The United Kingdom*, 44787/98, paras. 50–51; ECtHR, 28 April 2003, *Peck v. the United Kingdom*, 44647/98, para. 67.

[77] For example, police officers should refrain from entering a person's private home in order to prevent crime or disorder when this is highly unlikely to occur due to the absence of the person who was considered to potentially cause a breach of the peace. See in that regard for example ECtHR, 23 September 1998, *McLeod v. United Kingdom*, 72/1997/856/1065, paras. 56–57.

[78] ECtHR, 12 July 1988, *Schenk v. Switzerland*, 10862/84, paras. 49 and 53.

[79] ECtHR, 9 June 1998, *Teixeira de Castro v. Portugal*, 44/1997/828/1034, paras. 39 and 43.

[80] ECtHR, 4 October 2000, *Khan v. United Kingdom*, 35394/97, paras. 38–40.

[81] ECtHR, 16 December 1992, *Edwards v. United Kingdom*, 13071/87, para. 39; ECtHR, 26 October 1984, *De Cubber v. Belgium*, 9186/80, para. 30.

opportunity to challenge the evidence brought against him and the evidence is reliable and not gathered by means of entrapment or inducement, encroaching on the right to a private life can still produce admissible evidence.[82]

Taking all circumstances of the case into account, three considerations should be made. First, the evidence resulting from the breach of privacy should not be the only evidence in the case. In practice, no prosecutor would take the risk basing a whole case on such evidence, especially if this evidence would be open source data. Open source data are not necessarily reliable or accurate and would therefore have to be accompanied by other evidence. Second, the nature of the violation of the right to a private life should be considered. Evidence resulting from entrapment or incitement cannot lead to a fair trial due to its effect on the reliability of the evidence. No entrapment or incitement will be needed to collect open source data. Uncertainty regarding their accuracy and reliability is inherently linked to the make-up of open source data. Third, the right to challenge the evidence means that the person concerned should be given the opportunity to object to the use of such data as evidence implying that he or she needs to be informed of the use of these data.

IV.4. Personal Open Source Data in Criminal Investigations

IV.4.1. Accuracy and Reliability

Since open source data can theoretically be produced and distributed by any person, their accuracy and reliability is difficult to verify. When using such data for an investigation into a criminal offence or an offender, sufficient care should be taken to check source and content of the data. Law enforcement and intelligence authorities have implemented systems for verifying such data. Already in 1987 the CoE recognised the importance of these issues for police authorities in Recommendation (87)15. [83] With this recommendation, a group of experts drafted a special set of data protection principles for the specific tasks of the police while at the same time adapting them to take account of particular requirements, notably in respect of the suppression of criminal offences.[84]

The explanatory text of the recommendation rightfully states that the retaining of personal data in a police file may lead to a permanent record and indiscriminate storage of data, which may prejudice the rights and freedoms of the individual. It is also in the interests of the police that it has only accurate and reliable data at its disposal for the performance of its tasks. For these reasons, these guidelines encourage the implementation of a system of data classification; suggest distinctions between corroborated data and uncorroborated data, including assessments of human behaviour; between facts and opinions; between reliable information (and the various shades thereof) and conjecture; between reasonable cause to believe that information is accurate,

---

[82] ECtHR, 4 October 2000, *Khan v. United Kingdom*, 35394/97, para. 36.

[83] Council of Europe, *Recommendation No.R(87) 15 regulating the use of personal data in the police sector*, 17 September 1987, available online at <wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2> (accessed 1 October 2014).

[84] Even though this is not a legally binding instrument, it was explicitly endorsed in legally binding instruments covering police cooperation, such as the Europol Decision, the Schengen Implementation Convention as far as police cooperation is concerned, the Prüm Convention and the decision on the stepping-up of cross-border crime and the decision concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol.

and a groundless belief in its accuracy.[85] For example Europol has not only included Recommendation (87)15 in their standard of data protection,[86] the EU's agency for police cooperation also has a system in place for distinguishing incoming information based on its reliability.

In the current debates on the revision of the EU's data protection legal framework, the proposed directive for data protection in criminal matters included an additional provision on distinguishing personal data in accordance with their degree of accuracy and reliability. Also, the distinction between personal data based on facts and personal data based on personal assessments has been introduced in the text of the proposed directive.[87] Upon adoption of the proposed directive, making such distinction would then be mandatory for all data controllers processing personal data within the scope of this legal instrument.

IV.4.2. Necessity

Information will be collected for the purpose of a criminal investigation for a large part before a criminal charge is made; often it will be collected in order to make a criminal charge in the first place. This means that the protection of Article 6 ECHR is not activated yet, but the collected information can include data on suspects, witnesses as well as victims, and it can range from hard facts to suspicion and mere speculation. These can contain personal data so the data protection standards should apply. In most cases this would mean derogating from the standards as the use of personal data for criminal investigations will be an incompatible purpose as well as a possible breach of the data retention principle. Since derogating from the data protection standards is only lawful when it is laid down in law and necessary in the interests of – in this case – the suppression of criminal offences, the precise meaning of necessity in this respect deserves a closer look.

In the above explanation, necessity was referred to as the link between personal data and the purpose for which they are processed, in this case an investigation into one or more criminal offences. It does not explicitly require a criminal charge to be made, allowing a wider form of information—including proactive—gathering of personal data. Defining this link however, remains a nearly impossible task. In its assessment of the necessity of the mass retention of data in accordance with the Data Retention Directive the EU Court of Justice stated that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigative techniques. The Court continued nonetheless that such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention

---

[85] Council of Europe, *Recommendation No.R(87) 15 regulating the use of personal data in the police sector – Explanatory Memorandum*, 17 September 1987, para. 52, available online at <wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM> (accessed 28 November 2014).

[86] Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ L121/37, 15 May 2009, available online at <europol.europa.eu/sites/default/files/council_decision.pdf> (accessed 1 October 2014).

[87] European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)), 12 March 2014, available online at <europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0219> (accessed 1 October 2014).

measure such as that established by Directive 2006/24 being considered necessary for the purpose of that fight.[88] If the fight against serious crime is too wide to justify necessity, then a more specific link must exist. The 1987 CoE Recommendation regulating the use of personal data in the police sector gives further indications.[89] With regard to the collection of personal data, the recommendation defines the derogation regarding the suppression of criminal offences as the prevention of a real danger or the suppression of a specific criminal offence. "Real danger" should then be understood as not being restricted to a specific offence or offender but includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities.[90]

Translated into the issue of open source data, this means that it is a lawful exception to the data protection standards when open source data consisting of personal data are collected for the purpose of investigations into a specific criminal offence or offender, or in cases where a reasonable suspicion exists that one or more serious criminal offences have been or might be committed. Purely speculative collection of data—so-called fishing expeditions—does not concern necessary data collection and does not fall within the scope of the lawful derogation.

IV.4.3. Vigilantism

When discussing the topic of open source data and criminal investigations, the relatively recent trend of vigilantism using open sources on social media or the Internet should not be overlooked. What is meant by "vigilantism" or "vigilante justice" is a movement among citizens who take justice into their own hands and—often violently—react to alleged offenders out of discontent with law enforcement's action or lack thereof. Vigilantism in itself is not new, however it has been facilitated in recent years by the expansion of social media.

With estimates ranging from 80-90% of intelligence coming from open sources,[91] it is unsurprising that open sources are abused by persons outside the law enforcement and intelligence community. The fact that open source data are publicly available means that they are often viewed by the public as being used freely. This does not only have data protection violations as a consequence. Referring back to the aforementioned issue of

---

[88] Court of Justice of the European Union, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C 293/12 and C 594/12, para. 51.

[89] Council of Europe, *Recommendation No.R(87) 15 regulating the use of personal data in the police sector*, 17 September 1987, available online at <wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2> (accessed 1 October 2014).

[90] In the text of the recommendation a helpful example is added: reasonable suspicion that unspecified drugs were being illegally brought into a country through a port by unidentified private yachts would justify the collection of data on all such yachts using that port, but not all yachts, their owners and passengers using every port in that country. See Council of Europe, *Recommendation No.R(87) 15 regulating the use of personal data in the police sector*, 17 September 1987, available online at <wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2> (accessed 1 October 2014).

[91] Congressional Research Service, Best, R.A. and Cumming, A., *Open Source Intelligence (OSINT): Issues for Congress*, 5 December 2007, available online at <fas.org/sgp/crs/intel/RL34270.pdf> (accessed on 26 July 2014), 4.

accuracy and reliability of open source data, in cases of vigilantism, abusing such data can have fatal consequences.[92]

V. Reflections on Open Source Data

Open source data may appear, to the general public, as having an outlaw status and open to all kinds of use. This assumption is essentially incorrect. When open source data contain or consist of data that can identify or enable to identify an individual, they may not be used at free will. Even when the user is a law enforcement or intelligence officer doing his or her job to prevent or investigate a criminal offence, the data protection legislation should be complied with. Use of open source data for the suppression of criminal offences allows derogating from the personal data protection principles; nonetheless the following points deserve special attention.

Open source data are not necessarily verified, accurate or reliable. In comparison to already verified data, law enforcement and intelligence authorities have to invest more resources in organising, filtering and subsequently using open source data that are relevant for preventing and investigating criminal offences. The current revision of the EU's data protection legal framework makes the distinction of personal data based on different degrees of accuracy and reliability mandatory for data processing for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Collecting and processing open source data for targeted prevention and investigation into criminal offences constitutes a lawful derogation from the data protection standards. Mass or untargeted personal data collection, however, does not. Regardless of personal data being open source or closed source, the necessity and proportionality requirements apply.

A different light is shed on these data protection standards however by the ECtHR jurisprudence that has ruled on an independent relationship between the right to a private life and the right to a fair trial. When the person concerned had the opportunity over the course of the proceedings to challenge the evidence used against him, an interference with his privacy can still lead to a fair trial. Theoretically, this could endanger the necessity and proportionality requirements, also with regard to open source data. It is essential to closely monitor any future jurisprudence concerning this subject.

Open source data are available in vast amounts on account of the Internet and search engines such as Google, and they are tempting. In that sense, they are also unforgiving with regard to past mistakes and unfortunate life events. It may sound unfair to call this a "new reality", since the use of the Internet and social networks has increased for several decades already. However, the judicial and the legislative process are slow and cumbersome, or, to quote two privacy experts in a reaction to the judgment against Google: 'The CJEU decision is trying to balance things, perhaps assisting individuals a bit more than they deserve, until we all—Internet users, the Internet and Internet companies—get to better grips with the, still new, medium.'[93] On top of getting used to

---

[92] For example The Guardian, Morris, S., *Investigations opened into vigilante murder of man mistaken for paedophile*, 29 October 2013, available online at <theguardian.com/uk-news/2013/oct/29/vigilante-murder-paedophile-bristol-bijan-ebrahimi> (accessed on 26 July 2014).

[93] Privacy Perspectives, De Hert, P. and Papakonstantinou, V., *How the European Google Decision May Have Nothing To Do With a Right to Be Forgotten*, 19 June 2014, available online at <privacyassociation.org/news/a/how-the-european-google-decision-may-have-nothing-to-do-with-a-right-to-be/> (accessed 30 July 2014).

this relatively new reality, modernising the data protection legal framework is an undertaking with many stakeholders and diverging interests at stake. Legislators as well as judges are realising that the new questions that have surfaced need answers and by the time an answer has been found to one question, another issue will have appeared. The aftermath of the judgment against Google shows exactly how challenging this new reality is for those who perform a supervising role in it. It is of fundamental importance that in getting used to this new reality and adapting the existing legal framework to it, we do not lose touch with the data protection principles that have survived technological developments for several decades already.

The particular issues and questions that are triggered by the use of open source data warrant thorough and detailed reflection, although, this is not only the case for legislators and judges. Also the general public should reflect thoroughly on how to behave appropriately in this new reality. Prevention being the best cure, the simple awareness of what could happen once personal data are posted publicly can make a difference. This does not mean that the future of Internet and social media should come with a warning similar to the Miranda rights referred to in the title of this paper; it means that the debate on open source data should not only be held in parliaments and around congress tables but also in living rooms and around kitchen tables.

*

Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm

McKay Cunningham*

Keywords
INTERNET OF THINGS; PERSONAL INFORMATION; PRIVACY; PASSIVE DATA COLLECTION; DIRECTIVE

Abstract
The disparities inherent in various national privacy laws have come into sharper contrast as access to information grows and formerly domestic markets become international. Information flow does not adhere to national boundary lines. Increasingly, laws that seek to protect informational privacy do not either. The European Union took a bold approach by limiting access to its markets for those who failed to observe its strict law designed to protect personal information. The 1995 Directive (and 2014 Regulatory Amendment) embody this approach as they: (1) broadly define personal information; (2) broadly define those who process and control personal information; (3) restrict transfer of personal information to those who cannot demonstrate compliance. Tellingly, the Directive does not limit its scope to certain industries or practices, but requires privacy controls across the board, regardless of whether the processor is a healthcare provider, pastry chef or girl scout.

To many, the Directive has failed. While the global trend toward adopting laws similar to the Directive suggests that many States value privacy rights, commentators and empirical studies reveal significant shortcomings. The Directive outlaws harmless activities while allowing exceptions that threaten to swallow the rule. It is simultaneously over-inclusive and under-inclusive. National governments enjoy wide latitude to collect and use personal information under the guise of national security. Perhaps more concerning, technology continues to leapfrog. Information privacy is made continually more difficult with each new "app" and innovation. The Internet of Things is more probable than speculative. Radio-frequency identification is a predicate to computer identification and assimilation of everyday physical objects, enabling the use of these objects to be monitored and inventoried by computers. Tagging and monitoring objects could similarly be accomplished by other technologies like near field communication, barcodes, QR codes and digital watermarking, raising the legitimate argument that informational privacy—at least as envisioned in the 1995 Directive's absolute terms—is impossible.

Informational privacy cannot be accomplished by declaring it a fundamental right and outlawing all processing of personal information. To legally realise and enforce a privacy right in personal information, incremental, graduated, and practical legislation better achieve the goal than sweeping proclamations that have applications to actions unrelated to the harms associated with the absence of the right. With information privacy in particular, a capacious claim of right to all personal information undermines legal enforcement because the harms attending lack of privacy are too often ill-defined and misunderstood. As a result, legal realization of a claimed privacy right in the Age of Information should proceed incrementally and begin with the industries, practices, and

* Associate Professor, Concordia School of Law.

processes that cause the most harm by flouting informational privacy. Data mining and data aggregation industries, for example, collect, aggregate and resell personal information without express consent. A targeted prohibition of this industry would reduce financial incentives of the most conspicuous violators and alleviate some of the most egregious privacy infractions.

A graduated legal scheme also reduces undue and overbroad Internet regulation. While the right to privacy has been recognised and legally supported in one way or another for centuries, it has not faced the emerging and countervailing Age of Information until now. Current omnibus international legislation reflects the impossibility of legally protecting all privacy in the Age of Information; it also illustrates the need for a refined and practical legal scheme that gradually and directly targets the harms associated with privacy violations.

I. Introduction

Keeping our privacy is more unlikely than ever. Simply by moving from one place to another we exude data exhaust. This data exhaust, much of it personal, is valuable and increasingly collected without our knowing it. Everyday objects equipped with sensors that communicate to the Internet are commonplace and more are on the way. Over 200 billion worldwide are expected by 2020.[1]

Cisco projects that 'pretty much everything you can imagine will wake up.'[2] Already libraries tag and track every book in the collection,[3] dentists graft sensors into toothbrushes[4] and beer mugs with tilt sensors transmit consumption rates.[5] Smart phones, replete with apps that collect data exhaust, gather worlds of information like steps taken in a day, heartbeats per minute, driving logistics, hemoglobin, sleep habits and much more.[6] Rooftop video cameras, license plate readers, automobile GPS and smart phones log and report locational data by precise date and time.[7]

---

1 Time, Bajarin, T., *The Next Big Thing for Tech: The Internet of Everything*, 13 January 2014, available online at <time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/> (accessed 10 October 2014).

2 CISCO, *What is the Internet of Everything?*, available online at <cisco.com/web/tomorrow-starts-here/ioe/index.html> (accessed 10 October 2014).

3 Electric Engineering and Computer Science, Molnar, D., and Wanger, D., *Privacy and Security in Library RFID: Issues, Practices and Architectures*, 26–28 October 2004, available online at <cs.berkeley.edu/~daw/papers/librfid-ccs04.pdf> (accessed 11 October 2014).

4 Forbes, Clark, T., *At Mobile World Congress, A Connected Future Becomes Reality*, 27 February 2004, available online at <forbes.com/sites/sap/2014/02/27/at-mobile-world-congress-a-connected-future-becomes-reality/> (accessed 10 October 2014).

5 Wired, Thompson, C., *No Longer Vaporware: The Internet of Things is Finally Talking*, 6 December 2012, available online at <wired.com/2012/12/20-12-st_thompson/> (accessed 11 October 2014).

6 San Jose Mercury News, Boudreau, J., *Your phone, your life: New apps change how you use mobile devices*, 13 March 2009, available online at <mercurynews.com/ci_11900793?IADID=Search-www.mercurynews.com-www.mercurynews.com> (accessed 11 October 2014); Zamani, D., "There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones", *Hastings Constitutional Law Quarterly*, vol. 38, 2010, 174–175; Wall Street Journal, Thurm, S. and Kane, Y. I., *Your Apps Are Watching You*, 17 December 2011, available online at <online.wsj.com/news/articles/SB10001424052748704694004576020083703574602> (accessed 11 October 2014).

7 Pell, S., and Soghoian, C., "Can You See Me Now: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact", *Berkeley Technology Law Journal*,

While technology leapfrogs, legislation flags. Few laws regulate the collection of data exhaust and fewer still address how that data can be used. Given the expansion of sensors and the emergence of the Internet of Things, it is increasingly unlikely that a person can know precisely how much of her data is captured, who controls it and for what purpose.

Policymakers seeking to protect informational privacy face a daunting task. Information flow does not adhere to national boundary lines. As a result, the most effective privacy laws do not either. The European Union boasts the paragon of privacy laws by limiting access to its markets for those who fail to observe its strict law designed to protect personal information. By so doing, it bends international law into conformity.[8]

The EU 1995 Directive (and 2014 Regulation) embody this approach as it: (1) broadly defines personal information; (2) broadly defines who processes and controls personal information; (3) restricts transfer of personal information to those who cannot demonstrate compliance with the law's strictures.[9] The Directive does not limit its scope to certain industries or practices, but requires privacy controls across the board,[10] regardless of whether the data processor is a hospital, pastry chef or girl scout.

While the Directive is laudable in its omnibus effort to protect privacy, it fails in several significant aspects. The Directive outlaws harmless activities while it allows harmful exceptions that threaten to swallow the rule. It is simultaneously over-inclusive and under-inclusive. For example, it includes an employer gathering her or his colleagues' lunch orders and excludes data collected for "national security", a fluid concept undefined by the Directive.[11] The "national security" exception arguably allowed the US global surveillance programs, data mining, and third party data collection unveiled by Edward Snowden's revelations.[12]

The EU Directive also fails to protect against an equally ominous threat, albeit a threat less publically acknowledged: the Internet of Things. Everyday devices—objects—talk to one another online. Sensors connect objects to the Internet and enable the object to send, receive and analyse data automatically without human intervention. Outfitting innumerable objects with identifying and transmitting technology could be fundamentally transforming.

Privacy laws fail to address the loss of privacy through data exhaust and the Internet of Things. The EU Directive, for example, hinges on providing individuals with notice and obtaining their consent before collecting data, but the Internet of Things collects data without user awareness, to say nothing of notice and consent. The Directive fails to countenance the proliferation of indirect data collection, instead relying on the faulty

---

vol. 27, 2012; Rice, K.P., "You Are Here: Tracking Around the Fourth Amendment to Protect Smartphone Geolocation Information with The GPS Act", *Seton Hall Legislative Journal*, vol. 38, 2013.

8 Greenleaf, G., "Global data privacy laws: 40 years of acceleration", *Privacy Laws & Business International Report*, vol. 112, September 2011, 11–17.

9 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU 95/46/EC Directive).

10 *Ibid*.

11 Directive 95/46/EC, *supra* nt. 9, Article 3(2).

12 Lerner, J., Frank, M., Lee, M., and Wade, D., "The Duty of Confidentiality in the Surveillance Age", *Journal of Internet Law*, vol. 17, ed. 1, 2014; International New York Times, The Editorial Board, *Edward Snowden, Whistle-Blower,* 1 January 2014, available online at <nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?_r=0> (accessed 11 October 2014).

premise that users actively volunteer personal information and are aware when they divulge it.

This article posits that informational privacy cannot be accomplished by declaring it a fundamental right, outlawing all processing of personal information, and enforcing the law through notice and consent. To legally realise and enforce a privacy right in personal information, incremental, graduated, and practical legislation better achieve the goal than sweeping proclamations that have applications to actions unrelated to the harms associated with the absence of the right. With information privacy in particular, a capacious claim of right to all personal information undermines legal enforcement because the harms attending lack of privacy are too often ill-defined and misunderstood.

Regulating the *use* of sensitive data as it relates to particular risks or harms better comports with consumer law generally and allows needed adaptability to reflect context and changing technology. Calibrating the risk of harm from the use of data in a particular context reveals the value of that data and allows local regulatory regimes to incrementally adopt protective policies. An incremental risk-based approach is not a panacea and requires a normative taxonomy. But identifying and defining diverse data contexts and uses, and identifying the attendant risks or harms from the user's viewpoint are critical to successful implementation of contextual and harm-based personal data regulation.

In Part II, this article outlines the difficulty inherent in maintaining privacy in the Age of Information. Shortcomings stemming from the most prominent data privacy law are exposed, suggesting that the EU Directive is ineffective as both under and over-inclusive. Part III identifies an added difficulty, passive data collection and the Internet of Things. Personal data collected without user awareness is widespread now and will soon be ubiquitous. Current privacy laws, including the EU Directive, poorly address the collection and use of data generated without user awareness. Part IV urges policymakers to shift focus away from data collection and instead regulate data use. In particular, regulation should contextualise—from an individual's viewpoint—the privacy risks associated with an entity's purported use of that data. Legal realisation of a claimed privacy right in the Age of Information should proceed incrementally and begin with the industries, practices, and processes that cause the most harm by flouting informational privacy. Current omnibus international legislation reflects the impossibility of legally protecting all privacy in the Age of Information; it also illustrates the need for a refined and practical legal scheme that gradually and directly targets the harms associated with privacy violations.

II. Privacy in the Information Age

II.1. Deluge of Data

Never before has so much information been so readily available to so many.[13] In two decades from the commercialisation of the Internet in 1995[14] to today, Internet penetration has grown in exponential fashion.[15] From 2000 to 2012, Internet users grew from 360 million to 2.4 billion, a 566% growth rate.[16] As of 2012, 34% of the world population is connected.[17] In America, 66% of the adult population own at least one personal computer and 77% regularly use the Internet.[18]

While Internet penetration among many African nations ranks among the lowest, the growth rate—the rate of new Internet users in Africa—far eclipses the growth rates reported by the rest of the globe.[19] Some project that Internet traffic will grow by more than 50% in Latin America, the Middle East and Africa.[20] In one year alone, China added over 27 million Internet users.[21]

Not only is Internet access pullulating, the volume of information generated and transmitted is amplifying. One consultancy estimates that 2.8 zettabytes were created in 2012 and that by 2015 that number will double.[22] Facebook's 1.2 billion users generate an average of ninety pieces of content each month.[23] Wal-Mart reports more than one million transactions an hour, and YouTube estimates that every sixty seconds users

---

13 Mayer-Schönberger, V., and Cukier, K., *Big Data, A Revolution that Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt Publishing, 2013.

14 Frischmann, B., "Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market", *The Columbia Science and Technology Law Review*, vol. 2, 2001, 1–70.

15 Internet Usage Statistics, available online at <internetworldstats.com/stats.htm> (accessed 11 October 2014).

16 *Ibid.*

17 *Ibid.*

18 *Ibid*.

19 Engineering News, Esterhuizen, I., *Internet Growth Strong in Africa*, 16 January 2012, available online at <engineeringnews.co.za/article/Internet-growth-strong-in-africa-2012-01-16> (accessed 11 October 2014); Citizen, *Africa Internet Use Hits 2,000 Per Cent Growth*, 17 January 2012, available online at <thecitizen.co.tz/Business/-/1840414/1813774/-/iwlyg2/-/index.html> (accessed 11 October 2014).

20 Global Pulse, Blog, *Big Data for Development: Challenges & Opportunities*, May 2012, available online at <unglobalpulse.org/BigDataforDevWhitePaper> (accessed 16 November 2014). Global Pulse is a United Nations project, initiated in 2009 by the Secretary General. The UN tasked Global Pulse with exploring opportunities deriving from digital data in order to help policymakers evaluate crises in real time for vulnerable populations.

21 PC World, Kan, M., *China Reaches 485 Million Internet Users as Growth Slows*, 19 July 2011 available online at <pcworld.com/businesscenter/article/235978/china_reaches_485_million_internet_users_as_growth_slows.html> (accessed 11 October 2014); 'There is now so much data stored in the world that we're running out of language to describe it. The only quantity bigger than a zettabyte is a yottabyte, a figure with 24 zeroes.' International Bar Association, IBA Global Insight, Lowe, R., *Me, Myself and I*, 14 October 2013, available online at <ibanet.org/Article/Detail.aspx?ArticleUid=B47A1361-16DD-4F04-B83D-ADD60898F213> (accessed 11 October 2014).

22 MIT Technology Review, Tucker, P., *Has Big Data Made Anonymity Impossible?*, 7 May 2013, available online at <technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/> (accessed 11 October 2014).

23 Prasad, A., Mehta, K., Ventre, A., and Kearney, A. T., *Big Data: Understanding This New Normal*, 1107 PLI/Pat 411, 2012.

upload sixty hours of video.[24] Users send approximately 294 billion emails every day.[25] At 487 billion gigabytes, the world's digital content reduced to a stack of books would reach to Pluto ten times.[26] That is 'more than 1,000 gigabytes of data—twice the capacity of a standard laptop—of data for every person on earth in 2015.'[27] Given recorded human history, this near ubiquity of easy information over a mere twenty years is difficult to underestimate.

II.2. Threat to Privacy

This deluge of information threatens personal privacy, a fundamental right in many nations.[28] Ready access to individual's precise location,[29] tax returns,[30] Internet browsing history,[31] social interactions,[32] religious affiliation[33] and more carry a host of unwanted harms ranging from profiling by commercial marketers, [34] to undue governmental criminal investigation,[35] to health insurance rate increases,[36] to chilling political speech.[37]

One report from the 2014 World Economic Forum noted, 'The growth of data, the sophistication of ubiquitous computing and the borderless flow of data are all

---

24 *Ibid.*

25 *Ibid*.

26 The Guardian, Wray, R., *Internet data heads for 500bn gigabytes*, 18 May 2009, available online at <guardian.co.uk/business/2009/may/18/digital-content-expansion> (accessed 11 October 2013).

27 Liberty Global Policy Series, Boston Consulting Group, "The Value of Our Digital Identity", 2012, available online at <libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf> (accessed 10 December 2014).

28 Samuelson, P., "Privacy as Intellectual Property?", *Stanford Law Review*, vol. 52, 2000, 1125–1173; Loring, T. B., "An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States", *Texas International Law Journal*, vol. 37, 2002, 423–460.

29 Yakowitz, J., "Tragedy of the Data Commons", *Harvard Journal of Law and* Technology, vol. 25, 2011, 1–67.

30 Schwartz, P. M., "The Future of Tax Policy", *National Tax Journal*, vol. 61, 2008, 883–900.

31 McIntyre, J. J., "Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information", *DePaul Law Review,* vol. 3, 2011 895–936, 913.

32 Stoddart, J., "Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites", *Saskatchewan Law Review*, vol. 74, 2011, 263–274; Gunasekara, G., and Toy, A., "Myspace" or Public Space: The Relevance of Data Protection Laws to Online Social Networking", *New Zealand Universities Law Review*, vol. 23, 2008, 191–214.

33 Bergelson, V., "It's Personal But Is It Mine? Toward Property Rights In Personal Information"*, UC Davis Law* Review, vol. 37, 2003, 379–451.

34 DeMarco, D. A., Note, "Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood and Pragmatism, Pop-Tarts and Six-Packs", *Texas Law Review*, vol. 84, 2006, 1013–1065, 1019; McClurg, A. J., "A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling", *Northwestern University Law Review,* vol. 98, 2003, 63–144, 90–91 .

35 Kline, C., "Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute", *University of Toledo Law Review*, vol. 39, 2008, 443–495; Cockfield, A. J., "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance", *Queen's Law Journal*, vol. 29, 2003, 364–407.

36 Florencio, P. S., and Ramanathan, E.D., "Secret Code: the Need for Enhanced Privacy Protections in the United States and Canada to Prevent Employment Discrimination Based on Genetic and Health Information", *Osgoode Hall Law Journal*, vol. 39, 2001, 77–116.

37 Michelman, S., "Who Can Sue Over Government Surveillance?", *University of California Law* Review, vol. 57, 2009, 71.

outstripping the ability to effectively govern on a global basis.'[38] This point is worth emphasis: digital data knows no borders in the Internet age.[39] Metal file cabinets filled with paper dossiers and glossy photographs are of receding relevance. Digital data—including personal information—can be many places at once, travel thousands of miles in fractions of seconds from one nation to the next, and can be readily collected without notice or consent.[40] Digital data's fluid and borderless nature undermines national legislation aimed at regulating the collection and use of such information.[41] As one analyst put it, 'in the age of big data, those laws constitute a largely useless Maginot Line.'[42]

The difficulties inherent in national regulation of digital data are exacerbated by the diversity of data sources.[43] Digital data comes from everywhere: cell phone GPS signals, online browsing, cookies, digital purchases, social media pictures and posts, traffic videos and license plate cameras.[44] Emerging technologies like wearable devices will further the volume and variety of data input.[45] Google Glass, for example, collects, inventories, analyses and reports information that was previously intimate.[46]

Passive data sources are similarly emerging.[47] The Internet of Things—discussed in more detail below—imbues ordinary objects with in-product sensors that report activity through the Internet and relay usage data.[48] 'Automobiles, home appliances and energy meters are among the traditional product categories that have—or soon will have—integrated links to the internet,'[49] but this is only the beginning. In Europe, an additional seventy-five million objects will be connected to the Internet by 2015.[50] As the volume, variety and velocity[51] of digital data increases, so does the difficulty of implementing national legislation that effectively regulates it.[52]

---

38 World Economic Forum (WEF) prepared in collaboration with Kearney, A.T., *Rethinking Personal Data: A New Lens for Strengthening Trust*, May 2014, available online at <www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf> (accessed 13 October 2014); see Nguyen, C., and Haynes, P., "Rebalancing Socioeconomic Asymmetry in a Data-Driven Economy", *World Economic Forum Global Information Technology Report*, 2013.

39 Geist, M., "Cyberlaw 2.0", *Boston College Law Review*, vol. 44, 2003; Goldsmith J., and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World*, Oxford University Press, 2006, 188.

40 *Ibid*.

41 Steward, M. G., "Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet", *The Business Lawyer*, vol.55, 2000.

42 Mayer-Schonberger and Cukier, *supra* nt. 13, 16.

43 Yakowitz *supra* nt. 29,'Today, data privacy practices are shaped by some combination of ambiguous statutory directives, inconsistent case law, industry best practices, whim, and self-serving discretionary preferences. The time is ripe for the creation of uniform data privacy policies, and there is much to fix'.

44 Mayer-Schonberger and Cukier, *supra* nt. 13, 16.

45 Schwartz, P. M., "Property, Privacy and Personal Data", *Harvard Law Review*, vol. 117, 2004.

46 Wagner, M. S., "Google Glass: A Preemptive Look at Privacy Concerns", vol. 11, *Journal on Telecommunications & High Technology Law*, 2013; Wall Street Journal, Wilson, J. W., *Wearable Gadgets Transform How Companies Do Business*, 20 October 2013, available online at <online.wsj.com/news/articles/SB10001424052702303796404579099203059125112> (accessed 11 October 2014).

47 WEF and Kearney, *supra* nt. 38.

48 Lowe, *supra* nt. 21.

49 The Value of Our Digital Identity, *supra* nt. 27.

50 *Ibid.*

51 *Ibid*.

52 Lowe, *supra* nt. 21.

The most effective legislation, like the data it seeks to regulate, is itself borderless. The most widely acclaimed example is the European Union's 1995 Directive.[53] The Directive seeks to ensure citizen's rights to their personal information by truncating access to European markets for those who fail to comply with the Directive's strictures.[54] The Directive's effectiveness in large part stems from its extra-jurisdictional reach.[55] But the law has not succeeded. Where the Directive confronts the operose task of capturing transnational data flow, it fails in several other critical respects. This article posits that the Directive, laudable in aspiration, fails in practice. It is at once fatally over-inclusive and under-inclusive.

II.3. Leading Global Privacy Regulation: The European Union Directive

II.3.1. The Directive's Broad Scope

The Directive seeks to regulate the collection, storage, use, and dissemination of personal data;[56] it treats the right to privacy as a fundamental right,[57] awarding individuals autonomy over the distribution of personal data.[58] The Directive casts a wide net, illustrated by three key definitions. The Directive applies to (1) personal data, that is (2) processed by (3) controllers or processors.[59] Personal data is defined in the Directive as

> Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[60]

Personal data refers not just to names, national identification numbers, social security numbers and addresses but includes information that can lead to identification directly or indirectly.[61] This definition of personal data equates identified with identifiable.[62] Data is

---

53 Directive 95/46/EC, *supra* nt. 9; Lindsay, D., "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law", *Melbourne University Law Review*, vol. 29, 2005, 154–59.

54 "International Privacy Issues", 23 No. 3 *International Human Rights Journal*, Article 4, 2014.

55 Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000.

56 Murray, P. J., "The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?" *Fordham International Law Journal*, vol. 21, ed. 3, 1998, 932–1018, 933.

57 Sotto, L. J., *Privacy and Data Security Law Deskbook*, Aspen Publishers, New York, 2010, Section 18.02[A], '[t]hus the Data Protection Directive is based on internationally recognized fundamental human rights, specifically, the fundamental human right to privacy'.

58 Directive 95/46/EC, *supra* nt. 9, the Directive provides data subjects with a number of rights with respect to their personal data, including but not limited to: (1) the right of access to data; (2) the right to withhold permission to use data; (3) the right to have inaccurate data rectified; and (4) the right of recourse in the event of unlawful processing of data.

59 *Id.,* Articles 2, 6, 7.

60 *Id.,* Article 2(a).

61 *Ibid*.

62 Schwartz, P. M., and Solove, D. J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *New York University Law Review*, vol. 86, ed. 6, 2011, 1814–1894, 1819, arguing that information privacy regulations rest on an unstable and ill-defined concept of personally identifiable information.

considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot itself make the link.[63] As one EU authority stated, data is considered "personal" when, 'although the person has not been identified yet, it is possible to do it.'[64] Thus, information need not identify an individual directly to constitute "personal data", the mere fact that the information is related to an individual capable of being identified results in the data being "personal data" under the Directive.[65]

The Directive couples this broad definition of personal data with a broad definition of data "processing," defined as

> [A]ny operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[66]

Any collection, use and transfer of personal data—even the redaction and deletion thereof—constitutes "processing".[67] This definition purposefully includes data processed automatically as part of a filing system.[68] The Directive defines those deemed to have "processed" personal data as either data controllers or data processors. A data controller is 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.'[69]

Under these definitions, it is difficult to imagine commercial use of the Internet without processing personal information of some ilk. Given the law's broad reach and the significant restrictions levied on those that process personal information, policymakers anticipated that many organisations would sooner relocate or transfer processing functions overseas than comply.[70] The European Commission Website concedes the same: 'Without such precautions, the high standards of data protection established by the Data Protection Directive would quickly be undermined, given the ease with which data can be moved around in international networks.'[71]

The Directive's "precautions" include mechanisms that effectively legislate outside the jurisdiction of the European Union.[72] 'Because of its potential effect on other nations that interact with or do business in Europe, it may be the most controversial feature of the

---

63 *Id.*, 1817.

64 European Commission, Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 20 June 2007, available online at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> (accessed 17 October 2014).

65 Sotto, *supra* nt. 57, Section 18.02[A].

66 Directive 95/46/EC, *supra* nt. 9, Article 2(b).

67 *Ibid*.

68 *Id.*, Article 5, Recital 15.

69 *Id.*, Article 2(d).

70 Assey, J. M. Jr. and Eleftheriou, D. A., "The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?" *CommLaw Conspectus*, vol.9, ed. 2, 2001, 145–158, 146.

71 European Commission, *Transferring your personal data outside the EU*, 20 May 2014, available online at <ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm> (accessed 17 October 2014).

72 Sotto, *supra* nt. 57, Section 18.02[A]1[c].

Directive.'[73] One mechanism that forces international compliance does so through the use of "equipment" located in the EU.

> Each Member State shall apply … this Directive to the processing of personal data where: (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[74]

An EU company trying to avoid compliance with the Directive by relocating to Canada could not successfully do so if the personal data involved the computer, smart phone, or other such equipment of an EU resident. This provision not only dissuades EU companies from relocating, it also imposes the Directive's requirements on a host of non-EU entities. Many organisations headquartered in countries outside the European Union have been surprised to learn of their obligation to comply with EU law.[75]

The Directive's reach does not stop with data processing that uses EU-based "equipment",[76] it specifically targets data transfers to "third countries".[77] Article 25 prohibits the transfer of personal data to a third country (any Non-EU or EEA country) unless the European Commission deems that country "adequate".[78] The Commission currently recognises only twelve countries as adequate: Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay.[79] Given the broad definition of "personal information", the global economy and the free flow of data over the Internet, restricting data flow to twelve countries appears unmanageable at best.

Three principal avenues—outside a finding of nationwide adequacy—allow non-EU entities to receive and process EU personal data: (1) binding model contracts,[80] (2) binding corporate rules,[81] (3) Safe Harbor self-regulation.[82] The Directive also contains

---

73 Salbu, S. R., "Regulation of Borderless High-Technology Economies: Managing Spillover Effects", *Chicago Journal of International Law*, vol. 3, ed. 2, 2002, 137–153, 137; see also Kuner, C., "Beyond Safe Harbor: European Data Protection Law and Electronic Commerce", *The International Lawyer*, vol., 35, 79, 87.

74 Directive 95/46/EC, *supra* nt. 9, Article 4.

75 Salbu, *supra* nt. 73, 137.

76 Directive 95/46/EC, *supra* nt. 9, Article 25.

77 *Ibid*.

78 *Ibid*.

79 European Commission, *Commission decisions on the adequacy of the protection of data in third countries*, 24 June 2014, available online at <ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm> (accessed 17 October 2014), providing the requirements for "adequacy" and listing the few countries whose national laws meet the requirements.

80 Directive 95/46/EC, *supra* nt.9, Article 26(4); The Directive allows transfers of personal data even to third countries that fail to ensure an adequate level of protection if the data controller erects 'sufficient safeguards' via 'certain standard contractual clauses' consistent with a 'Commission's decision'. Under this approach, the contractual clauses incorporate by reference the data protection law of the Member State in which the data exporter is established. See Leathers, D. R., "Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions for Effective Enforcement" *Case Western Reserve Journal of International Law* vol. 41, ed.1, 2009, 193–242, 199–200.

81 Directive 95/46/EC, *supra* nt.9, Article 29, binding corporate rules track EU data protection standards and allow multinational organisations to conduct business with EU counterparts without having to draw up model contract language for every transaction. The relevant Member State's Data Protection Agency must approve binding corporate rules, which can be an arduous and lengthy process. As a

situational exceptions and derogations that allow processing of personal data and often undermine the law's broad definitions and extra-jurisdictional reach.[83] The Directive, despite its worthy aspiration, contains significant shortcomings. It is both over and under-inclusive.

II.3.2. The Directive's Over-Inclusiveness

By most accounts, protecting personal information is a deserving goal. The Directive's extra-jurisdictional reach, penalties for non-compliance, and expansive definition of those who process personal information reflect sincerity in reaching that goal.[84] Ironically, by purporting to protect all personal information from almost all processing, the Directive undermines its central objective; its over-inclusiveness debilitates its effectiveness.

II.3.2.1. Restricting Harmless Data Processors

Privacy scholar, Fred Cate, notes that children recording orders for Girl Scout cookies, individuals organising their business contacts, and students operating websites that require registration all qualify as data controllers under the Directive. 85 A co-ed collecting names for intramural flag football in Boise, Idaho is likely a "controller" who "processes" "personal information". Perhaps more commonly,

> anyone who posts personal information about another person on his or her own social networking profile or uses personal information from another

---

result, relatively few binding corporate rules have been approved. See Sotto, *supra* nt. 57, Section 18.02[B].

82 US Department of Commerce, *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 4 August 2014, available online at <export.gov/safeharbor/> (accessed 17 October 2014).

83 Directive 95/46/EC, *supra* nt. 9, art. Article26(1), the Directive's Article 26(1) authorises a number of other exceptions to legally transmit personal data outside of Europe even to a 'third country' that fails to offer an 'adequate level of protection'. A data controller or processor can legally send personal data outside of Europe to the United States, or any other country, if:

(a) the data subject has [freely] given his consent unambiguously to the proposed transfer [to be enforceable, a consent must indeed be unambiguous and freely given; EU data authorities take the position that a consent must specifically list the categories of data and the purposes for the processing outside the EU; in the employment context, consents may be deemed presumptively not freely given, merely because of the imbalance in bargaining power between employer and employee]; or

(b) the transfer is necessary [not merely convenient] for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary [not merely convenient] for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary [not merely convenient] or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary [not merely convenient] in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

84 Directive 95/46/EC, *supra* nt. 9.

85 Cate F. H., "The Changing Face of Privacy Protection in the European Union and the United States" *Indiana Law Review*, vol., 33, 1999, 173–232, 183.

> person's profile could be deemed a 'data controller' subject to the data protection obligations of the Directive.[86]

Seemingly innocuous data like the nine-digit numerical label assigned to each device that participates in a computer network amounts to personal data.[87] The Working Party on data privacy for the European Commission confirmed that IP addresses and cookies are "personal data",[88] a finding echoed by the US Federal Trade Commission in its proposed revisions to COPPA.[89]

In short, the Directive's broad reach captures an uncomfortably high percentage of "data processors" whose use of "personal information" is disassociated from the harm that the Directive seeks to alleviate.[90] As noted above, "personal information" under the Directive includes information that identifies a person and information that could lead to identifying a person. The EU Directive is not alone in using such a broad definition. The US Health Insurance Portability and Accountability Act defines identifiable health information as including information 'with respect to which there is a reasonable basis to believe the information can be used to identify the individual.'[91] In fact, the clear majority of nations that have enacted universal privacy laws regulate information that could lead to identification.[92]

This definition has proven increasingly problematic because most information that relates to a person—even when scrubbed to create "anonymity"—can be decoded.[93] 'The emergence of powerful re-identification algorithms demonstrates … the fundamental inadequacy of the entire privacy protection paradigm based on "de-identifying" the data.'[94]

Companies that collect personal information, like online retailers or social networking entities, often promise to share only customer information that is non-personally

---

86 Bennett, S. C., "The "Right to be Forgotten": Reconciling E.U. and U.S. Perspectives", *Berkeley Journal of International Law*, vol., 30, ed., 1, 2012, 161–195, 186.

87 McIntyre, J. J., "Comment, Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information", *DePaul Law Review*, vol. 60, ed. 3, 2011, 895–936, 897.

88 European Commission, Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, 00737/EN/WP148, 4 April 2008, 3, 8, available online at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf> (accessed 17 October 2014) (WP148).

89 Black J. E. Jr., "Privacy Liability and Insurance Developments in 2012*", Journal of Internet Law*, vol. 16, ed. 9, 2013, 3–13.

90 Yakowitz, *supra* nt. 29, noting unintended costs like preventing use of personal data to confront public health issues, create economic value, and prevent fraud); MIT Technology Review, Simonite, T., *Business Report—Big Data Gets Personal: Smartphone Tracker Gives Doctors Remote Viewing Powers*, 17 May 2013, available online at <technologyreview.com/news/514756/smartphone-tracker-gives-doctors-remote-viewing-powers/> (17 October 2014); MIT Technology Review, Talbot, T., *Business Report—Big Data Gets Personal: African Bus Routes Redrawn Using Cell-Phone Data*, 30 April 2013, available online at <technologyreview.com/news/514211/african-bus-routes-redrawn-using-cell-phone-data/> (accessed 17 October 2014)

91 Health Insurance Portability and Accountability Act, United States of America, 1996 as in force on 23 March 2010, US Code Title 42 Chapter 7(XI) Part C Section1320d (6)(B)(ii), available online at <law.cornell.edu/uscode/text/42/1320d> (accessed 17 October 2014).

92 Greenleaf, *supra* nt. 8, 11.

93 Ohm, P., "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review*, vol. 57, ed. 6, 2010, 1701–1777.

94 Narayanan, A. and Shmatikov, V., "Privacy and Security Myths and Fallacies of "Personally Identifiable Information", *Communications of the ACM*, vol. 53, ed. 6, 2010, 24–26.

identifiable.[95] Such promises will soon be illusory: 'They fundamentally rely on the fallacious distinction between "identifying" and "non-identifying" attributes.'[96]

By illustration, hackers recently employed content search queries to re-identify AOL customers. Location data, commercial transactions and web browsing history readily populate de-anonymising algorithms. Even movie-viewing histories have been shown to effectively re-identify users.[97] Combining the vast continuum of human characteristics and activities with the quantity and specificity of information already available, suggests that re-identification is inevitable and, more importantly, that 'any attribute can be identifying in combination with others.'[98]

Despite a high likelihood of re-identification, the concept of 'personally identifiable information' remains central to existing privacy regulations,[99] leading many to decry the use of 'personally identifiable information' as a regulatory lynchpin.[100] As discussed in more detail below, emerging technologies stretch the already broad applicability of such laws to near universality, revealing the over-inclusiveness and also arguably, the ineffectiveness of the EU Directive.

Moreover, enforcement of laws, that incriminate a disproportionately large ratio of those individuals governed by it, or that are so broad as to capture the entire body politic have historically been declared invalid. Criminalising those who speak in an "annoying" way,[101] or outlawing "vagrancy",[102] confer upon government *carte blanche* enforcement authority. Officials can arbitrarily choose to prosecute disfavoured parties. The Directive attracts similar criticism.[103]

Upset by lacklustre enforcement in the United States, for example, European Union officials chastised their US counterparts,[104] issuing a working paper noting that 'less than half of organisations post privacy policies' and that most failed to observe 'the expected

---

95 Ohm, *supra* nt. 93; Wall Street Journal, Steel, E. and. Fowler, G. A., *Facebook in Privacy Breach*, 18 October 2010, available online at <online.wsj.com/news/articles/SB10001424052702304772804575558484075236968> (accessed 17 October 2014).

96 Narayanan and Shmatikov, *supra* nt. 94.

97 *Ibid*.

98 *Ibid*.

99 Greenleaf, *supra* nt. 8.

100 Word Press, Taylor, L., *Hacking a Path Through the Personal Data Ecosystem*, 12 December 2013, available online at <linnettaylor.wordpress.com/2013/12/12/hacking-a-path-through-the-personal-data-ecosystem/> (accessed 17 October 20).

101 *People v Raphael Golb*, 2014 NY Slip Op 03426, Decided on May 13, 2014 Court of Appeals Abdus-Salaam, J. Published by New York State Law Reporting Bureau pursuant to Judiciary Law, Section 431; *People v Dietze* 75 NY2d 47 (1989), striking down a similar harassment statute, former Penal Law, Section 240.25, which prohibited the use of abusive or obscene language with the intent to harass, annoy or alarm another person; NY Times, Leland, J., *Top Court Champions Freedom to Annoy*, 13 May 2014, available online at <nytimes.com/2014/05/14/nyregion/top-court-champions-freedom-to-annoy.html?_r=0> (accessed 17 October 2014).

102 *Papachristou v Jacksonville*, 405 US 156 (1972); *Kolender v Lawson* 461 US 352 (1983), striking laws against vagrancy for unconstitutional vagueness; in restricting activities like 'loafing', 'strolling', or 'wandering around from place to place', the law gave arbitrary power to the police and, since people could not reasonably know what sort of conduct is forbidden under the law, could potentially criminalize innocuous everyday activities.

103 Leathers, *supra* nt. 81, 195–200.

104 *Ibid*, '[s]ince the Safe Harbor's inception, the program has been subject to heavy criticism from privacy advocates and an EU oversight committee. The heaviest criticism is levied against the Safe Harbor's inadequate internal and external enforcement mechanisms.'; US Federal Trade Commission, *Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics,* PRESS RELEASE, *6 August 2009*, available online at <ftc.gov/opa/2009/08/bestpriced.shtm> (accessed 17 October 2014).

degree of transparency as regards their overall commitment or as regards the contents of their privacy policies.'[105] Indeed, the FTC waited nine years before bringing a data privacy enforcement action;[106] the ambitious and over-inclusive nature of the Directive invites its arbitrary enforcement.

The Directive's over-inclusive model implicates another topic of note—data security. Security breaches from malware, hackers, netbots, viruses and all manner of cyber threats plague individuals and organisations alike. In April 2011, Sony suffered a massive breach in its video game online network.[107] Volumes of customer data were compromised, including names, addresses, and possibly credit card data associated with over seventy-seven million user accounts.[108] In 2005, America's major newspapers headlined the following: "Info Theft Slams Chain: 1.4 Million Card Numbers Stolen"; "Poll Says Identity Theft Concerns Rose After High-Profile Breaches"; "Data Security Breaches Alarm Consumers".[109] Data security experts recorded 403 million variants of malware in 2011.[110] As one commentator notes, '[s]cholars, government officials, journalists, and computer scientists all agree that inadequate security is an emerging threat—perhaps a catastrophic one…'.[111] Data that cannot be protected cannot be private.

Even so, the Directive includes no exception allowing data to be processed solely for security purposes.[112] Modern security protocols require analysis of massive data sets.[113] Anomalies in data usage often reveal cyber attacks.[114] In 2011, for example, a firm specialising in international money transfers notified authorities when it spotted a slight abnormality in Discover Card transactions originating in New Jersey.[115] Individually, the transactions appeared pedestrian, but viewed together and in context with large data sets,

---

105 European Commission, Commission Staff Working Paper, The Application of Commission Decision 520/2000/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, SEC (2002) 196, 13 February 2002, available online at <ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf> (accessed 17 October 2014)

106 Leathers, *supra* nt. 80, 195–196.

107 Kuhlmann, S., "Do Not Track Me Online: The Logistical Struggles Over the Right "To Be Let Alone" Online", *De Paul Journal of Art, Technology & Intellectual Property Law*, vol. 22, 2011, 242–245.

108 *Ibid*.

109 Barnes, M. E., "Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive", *Northwestern Journal of International Law & Business*, vol. 27, ed. 1, 2006, 171–198.

110 Symantec, *Internet Security Threat Report: 2011 Trends*, 12 April 2012, available online at <symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf> (accessed 29 October 2014).

111 Bambauer, D. E., "Conundrum", *Minnesota Law Review*, vol. 96, 2011, 584–674.

112 Data Protection Directive, *supra* nt. 8; but see Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM, 2012, 11 final, 25 January 2012. (Recital 39 of the new Regulation suggests there will be more room for security providers to process data).

113 Symantec, *Technology: Defense in Depth*, available online at <symantec.com/about/profile/star_technology.jsp> (accessed 29 October 2014), 'Network-based protection is a set of technologies designed to block malicious attacks before they have a chance to introduce malware onto a system. Unlike file-based protection, which must wait until a file is physically created on a user's computer before scanning it, network-based protection analyzes all incoming data streams before they can processed by the computer's operating system and cause harm'.

114 *Ibid*.

115 Mayer-Schonberger and Cukier, *supra* nt. 13, 27–28.

the irregularities revealed that the transactions came from the same criminal organisation. 'The only way to spot the anomaly was to examine all the data'.[116]

But those providing data security must comply with the Directive if the security measures require the "processing" of "personal data."[117] Given the massive data sets required by modern security programs, the likelihood of processing personal information is high.[118] For example, in 2012 Microsoft announced plans to publish a real-time intelligence feed drawn from its extensive data security protocols.[119] However, because the intelligence feed distributed IP addresses of systems infected by malware, the Directive posed a substantial obstacle.[120] Analysing and sharing large amounts of information is critical to data security, a task made onerous by the Directive's sweeping application. In choosing an ambitious scope, EU policymakers failed to account for the fact that safeguarding networks from hacking and cyber threats is itself a form of privacy protection.

II.3.3. The Directive's Under-Inclusiveness

While the Directive's over-inclusive scope encircles those whose use of "personal information" is removed from the harm that the Directive seeks to alleviate, it is simultaneously under-inclusive, ignoring many of privacy's worst offenders. Several exceptions and derogations threaten to outstrip the law's prime objective.[121] As a preliminary matter, the Directive does not have literal effect on Member States but only requires them to pass legislation that tracks the Directive in spirit and result.[122] Each Member State retains discretion as to form and implementation of the national privacy law that each ultimately enacts and enforces.[123] 'A margin for manoeuvre' potentially subverts the Directive by allowing disparate and inconsistent laws among Member States.[124]

More to the point, the Directive itself allows for specific exceptions, some of which are generally identified without limiting language. This article does not attempt to address them all. Two exceptions sufficiently reflect the Directive's failure to regulate many of the most harmful offenders: (1) the National Security and Criminal Proceedings exception;[125] and (2) the Safe Harbor exception.[126]

---

116 *Ibid*.

117 Cunningham, M, "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law", *George Washington International Law Review*, vol. 44, 2012, 643–696, 681–685.

118 *Ibid.*

119 Network World, Neagle, C., *Microsoft to Launch Real-Time Threat Intelligence Feed*, 12 January 2012, available online at <networkworld.com/news/2012/011212-microsoft-intelligence-254846.html> (accessed 29 October 2014).

120 Cunningham, *supra* nt. 117, 643–696.

121 Directive 95/46/EC, *supra* nt. 9, Articles 13, 26.

122 Directive 95/46/EC, *supra* nt. 9, Articles 22–23.

123 Sotto, *supra* nt. 57, Section 18.02.

124 Ritter, J. B., Hayes B. S. and Judy H. L., "Emerging Trends in International Privacy Law", *Emory International Law Review*, vol. 15, 2001, 87–92, nt. 11.

125 Directive 95/46/EC, *supra* nt. 9, Articles 3(2), 13.

126 European Commission, 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, available online at <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0518> (accessed 25 November 2014).

II.3.3.1. National Security Exception

Although national security and criminal investigations often require efficiency and secrecy, the Directive's drafters declined to define the scope of these exceptions.[127] National security is a fluid concept. The Directive predates the attacks of September 11, 2001 and the subsequent and ongoing war on terror.[128] Edward Snowden's revelations about US global surveillance programs, data mining, interception projects, third party data collection and complex analytic schemes unveiled privacy violations on a scale previously unknown.[129] The war on terror catalysed these invasive and covert programs, and the Directive's generalised exceptions for "national security", facilitate these open-ended and continuing privacy violations.[130]

The United States is not alone in its use of national security to boost data collection, analysis and retention. Many States have documented pervasive deprivation of privacy rights justified, in part, by national security.[131] A report given at the World Economic Forum noted the atmosphere of anxiety and agitation that often prevails, leaving a 'one-dimensional debate…where the interest of privacy are traded off against public safety and security'.[132] A better balance is required. The first data protection commissioner in the German State of Hesse argued that an individual's right to access should 'never be totally excluded, but rather can at most be partially restricted or temporarily suspended in a series of unequivocally defined and exhaustively listed cases'.[133] The Directive offers no such parameters, leaving government surveillance unregulated.

II.3.3.2. Safe Harbor Exception

The other notable exception is the Directive's Safe Harbor provision.[134] Unique to the United States and perhaps owing to its singular economic status at the time, the European Commission fashioned a heavily diluted version of the Directive for application to US entities that chose it.[135] The hope was to construct a streamlined channel for US entities to roughly comply with the Directive's strictures.[136] The watery version reflects US resistance to omnibus privacy legislation and ultimately signals to US entities that pro forma compliance suffices.[137]

Importantly, Safe Harbor facilitates hollow compliance because it is voluntary, self-certifying, and largely unenforced.[138] US businesses that process EU personal data

---

127 Directive 95/46/EC, *supra* nt. 9, Article 3(2), 13.

128 Directive 95/46/EC, *supra* nt. 9.

129 International Bar Association, IBA Global Insight, Mulrenan, S., *Snowden NSA Revelations Make Mockery of Hong Kong Resolve on Privacy*, August 2013.

130 Fitzgerald, E. O., "The Globalized Rule of Law and National Security: An Ongoing Quest for Coherence", *University of New Brunswick Law Journal*, vol. 65, 2014, 40–85.

131 *Ibid.*

132 WEF and Kearney, *supra* nt. 38; Nguyen, C. and Haynes, P., "Rebalancing Socioeconomic Asymmetry in a Data-Driven Economy", *in*: Bilbao-Osorio, B., Dutta, S. and Lanvin, B. eds., *Global Information Technology Report 2014: Rewards and Risks of Big Data*, Insight Report, World Economic Forum and INSEAD, 2014.

133 The Value of Our Digital Identity, *supra* nt. 27, 10.

134 European Commission 2000/518/EC Decision, *supra* nt. 126.

135 *Ibid*.

136 Cunningham, M., "Diminishing Sovereignty: How European Privacy Law Became International Norm", *Santa Clara International Law Journal*, vol. 11, 2013, 421–452.

137 *Id*., 440.

138 Wang, M.-L., "Information Privacy in a Network Society: Decision Making Amidst Constant Change", *National Taiwan University Law Review*, vol. 5, 2010, 127–154, 133 nt. 23.

regulate their own adherence to Safe Harbor privacy principles.[139] No government official reviews and then authorises whether any given company in fact complies with Safe Harbor principles before awarding certification.[140] An entity need only notify the US Department of Commerce that it intends to comply with Safe Harbor and publicly declare compliance on its website.[141] A US organisation that self-certifies through Safe Harbor is then afforded automatic approval from data processing authorities in the European Union.[142] Among US companies, this approach does not foster recognition and adherence to the privacy principles laid out in the Directive.[143] Neither does the relaxed approach incent US businesses to self-certify, as many view self-certification as creating unnecessary liability and oversight.[144] Professor Joel R. Reidenberg concludes that 'self-regulation is not an appropriate mechanism to achieve the protection of basic political rights. Self-regulation in the US reduces privacy protection to an uncertain regime of notice and choice.'[145]

Moreover, Safe Harbor certification shifts the jurisdiction from EU authorities to the US Department of Commerce and the Federal Trade Commission (FTC).[146] Although implemented in 2000, the FTC did not bring an enforcement action under Safe Harbor until 2009.[147] As one commentator notes, 'The heaviest criticism is levied against the Safe Harbor's inadequate internal and external enforcement mechanisms.'[148] In light of the large numbers of US organisations engaged in e-commerce or otherwise processing large amounts of data, the Safe Harbor "exception" effectively insulates a significant faction of privacy offenders.

The Directive aspires to protect privacy as a fundamental right regardless of industry, sector or other such context.[149] In so doing, it propagates a disconnect between the law and the harm it seeks to mitigate. By including almost all data processors irrespective of whether they cause privacy harms and by excluding those data processors that in fact harm individuals by misusing their private data, the Directive undermines its central objective.

---

139 Leathers, *supra* nt. 80, 196; Vitale, A., "The EU Privacy Directive and the Regulating Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet", *Vanderbilt Journal of Transnational Law*, vol. 35, 2002, 321–357, 339.

140 *Ibid.*

141 *Ibid.*; Sotto, *supra* nt. 57 , Section 18.02 [A], 2010.

142 *Ibid*; Rubinstein, I. S., "Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes", *I/S: A Journal of Law and Policy for the Information Society*, vol. 6, ed. 3, 2011, 355–423.

143 Reidenberg, J. R., "Setting Standards for Fair Information Practice in the U.S. Private Sector", *Iowa Law Review*, vol. 80, 1995, 497–551, 500, 'Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector. Legal rules have developed on an ad hoc, targeted basis, while industry has elaborated voluntary norms and practices for particular problems. Over the years, there has been an almost zealous adherence to this ideal of narrowly targeted standards.'

144 Nijhawan, D. R., "The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States", *Vanderbilt Law Review*, vol. 56, ed. 3, 2003, 940–996, 975–976, noting that 'in order to comply, companies must incur substantial costs to ensure that their data management processes meet threshold requirements'.

145 Reidenberg, J. R., "E-commerce and Trans-Atlantic Policy", *Houston Law Review*, Vol. 38, 2001, 717–750.

146 Cunningham, *supra* nt. 117, 681.

147 Sotto, *supra* nt. 57, Section 18.02[B].

148 Leathers, *supra* nt. 80, 195–196.

149 Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000, 1–88.

III. Next Generation Privacy

Protecting privacy through omnibus legislation like the EU Directive is unlikely to succeed.[150] Even universal international accord memorialised by a treaty purporting to protect informational privacy would likely fail because it misperceives the current era of big data—one that is firmly rooted and not easily upended by absolutist privacy legislation.[151]

III.1. Commercialisation and Ubiquity of Personal Data

The enormous amount of information already available allows easy re-identification; 'any attribute can be identifying in combination with others'.[152] A 2,000% increase in global data is expected by 2020.[153] The more data there is, the less that any of it can be said to be private.[154] Users continue to reveal personal data through social networking sites.[155] Such websites are growing three times faster than the overall Internet rate, and currently represent the fourth most popular online activity.[156] In other words, active data sharing is not slowing and those who seek privacy are often those who broadcast personal information in the digital world.[157] Perhaps fooled by the myth of online anonymity,[158] users continuously divulge bits of themselves when searching Google, purchasing items online, posting pictures, "liking" restaurants and browsing vacation spots.

These online actions appear free; they are not.[159] As computer scientist, Jaron Lanier writes: 'the dominant principle of the new economy, the information economy, has lately been to conceal the value of information'.[160] Google receives more than three billion search inquiries every day—and saves them all.[161] A recent study predicts 'the Big Data market is on the verge of a rapid growth spurt that will see it top the USD50 billion mark

---

150 Wang, *supra* nt. 138, 133 nt. 23.

151 Foreign Affairs, Mundie, C., *Privacy Pragmatism,* March-April 2014, available online at <foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism> (accessed 29 October 2014), 'Today, the widespread and perpetual collection and storage of personal data have become practically inevitable.'

152 Narayanan and Shmatikov, *supra* nt. 94.

153 Tucker, *supra* nt. 22, 2–3.

154 *Ibid.,* quoting Princeton University computer scientist, Arvind Narayanan; Mundie, *supra* nt. 151; but see Yakowitz, *supra* nt. 29, arguing that re-identification is not easy and that the digital commons is beneficial to scientific research.

155 Nielesen Online, *Social Networks & Blogs Now 4th Most Popular Online Activity, Ahead of Personal Email, Nielson Reports,* NEWS RELEASE, 9 March 2009, available online at <nielsen-online.com/pr/pr_090309.pdf> (accessed 29 October 2014) (Nielsen News Release); see also Neilsen Online, *Social Networking and Blog Sites Capture More Internet Time and Advertising*, Newswire, 24 September 2009, available online at <nielsen.com/us/en/insights/news/2009/social-networking-and-blog-sites-capture-more-internet-time-and-advertisinga.html> (accessed 29 October 2014); Nunziato, D. C., "Romeo and Juliet Online and in Trouble: Criminalizing Depictions of Teen Sexuality (c u l8r: g2g 2 jail)", *Northwestern Journal of Technology and Intellectual Property*, vol. 10, ed. 3, 2012, 57–92, 58.

156 *Ibid.*

157 Waldman, A. E., "Durkheim's Internet: Social and Political Theory in Online Society", *New York University Journal of Law and Liberty*, vol. 7, ed. 2, 2013, 345–440.

158 *Ibid*.

159 Lowe, *supra* nt. 21.

160 Lanier, J., *Who Owns the Future?*, Simon and Schuster, New York, 2013, 15.

161 Mayer-Schonberger and Cukier, *supra* nt. 13, 2.

worldwide within the next five years.'[162] Acxiom, a data wholesaler, maintains an average of 1,500 pieces of information on more than 500 million consumers across the globe.[163] 'Data collection is the dominant activity of commercial websites. Some 92% of them collect personal data from web users, which they then aggregate, sort, and use.'[164]

Facebook's value is not the number of people it can reach for advertisements but the volume and specificity of personal information it has on each Facebook user.[165] One Facebook user, after repeatedly asking Facebook to remit his personal data, eventually received more than 1, 220 pages of his personal information after only three years using Facebook.[166] 'Pictures uploaded from smartphones included precise global positioning system coordinates, the identities of anyone tagged in the photos and the moment—down to the second—when the shutter clicked. Information that users thought they had deleted survived in Facebook files.'[167]

Data analytics was an estimated USD25.1 billion industry in 2004 and a USD105 billion industry in 2010.[168] A 2010 study by IBM reveals that 83% of business leaders identify analytics as a top priority for their businesses.[169] The revenues of the largest data-mining companies exceed USD1 billion annually,[170] suggesting that the data collection and retention infrastructure is far-reaching, diverse and entrenched. Data and personal information were described in the World Economic Forum as 'the new oil'.[171]

The commercialisation of personal data, the myth of anonymity and the public's habitual reliance on the Internet stand in the way of omnibus privacy reform. Even in the unlikely event that users stop actively divulging personal information, and that legislation can uproot businesses whose revenue flow from collection and dissemination of personal data, "passive" data transmission and collection continue to grow with emerging technologies.

III.2. Emerging Technology and Passive Data Transmission

Broad privacy laws that regulate the collection and retention of personal information fail to account for new technologies and expanding sources of passive data generation. National privacy laws like the Directive presume the individual's voluntary participation, including the opportunity to consent to the collection of their personal information.[172]

---

162 Wikibon, Kelly, J., *Big Data Market Size and Vendor Revenues*, 3 January 2014, available online at <wikibon.org/wiki/v/Big_Data_Market_Size_and_Vendor_Revenues> (accessed 29 October 2014).

163 Tucker, *supra* nt. 22, 2–3.

164 Peppet, R. S., "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future", *Northwestern University Law Review*, vol. 105, 2011, 1153–1204, 1164.

165 New York Times, Sengupta, S. and Rulsi, E., *Personal Data's Value? Facebook Is Set to Find Out,* 31 January 2012, 'More than the world's largest social network, it is a fast-churning data machine that captures and processes every click and interaction on its platform'.

166 The Washington Post, Tmberg, C., *Austrian student challenges Facebook's use of personal data*, available online at <independent.co.uk/news/world/europe/austrian-student-challenges-facebooks-use-of-personal-data-8219155.html> (accessed 29 October 2014).

167 *Ibid*.

168 McClurg, *supra* nt. 34, 71–72.

169 Economic Times, *IBM Sees Biz Analytics Market Growing Sharply*, 11 May 2010, available online at <articles.economictimes.indiatimes.com/2010-05-11/news/27589148_1_business-analytics-information-integration-ibm-software-group> (accessed 29 October 2014).

170 McClurg, *supra* nt. 34, 71.

171 Lowe, *supra* nt. 21.

172 Directive 95/46/EC, *supra* nt. 9, Article 14(b), requiring that individuals 'be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing, and to be

But our data exhaust is increasingly collected without our awareness.[173] The proportion of personal data passively generated is growing and may even surpass personal data that is "actively" produced or volunteered by individuals.[174] Passively generated personal data can be further broken down into observed and inferred data.[175]

Observed data that is passively generated refers to data captured by recording individuals' activities.[176] Observed data is often, though not always, accompanied by the individual's unawareness of data collection.[177] While an individual may be aware that a browser cookie collects personal information, other forms of observational data elude awareness like rooftop security cameras and event data recorders that are found in most automobiles. In both instances, however, the individual does not proactively volunteer the information.[178] Importantly and perhaps ironically, the individual's lack of awareness and voluntariness tends to shift "ownership" and consequently control of the data to the entity that captured it.[179]

Inferred data, while similar to observed data, is differentiated by synthesis or analysis.[180] Through analysis of varying data, larger institutions create inferred data at a higher expense for predictive purposes.[181] Aggregation and analysis of multiple data points characterise inferred data.[182] Like observed data, inferred data suggests that it is the entity rather than the individual who exercises ownership and control. Especially given the novelty of the analysis, and the time and expense incurred creating it.[183]

Mobile phones provide a good example of passively generated data. Mobile phone companies track and record the location of the world's six billion mobile phone users.[184] Users do not voluntarily and constantly log and submit locational data. Locational data is intensely powerful.[185] On a micro level, for example, doctors can track the movement of diabetes patients, raising alarms for unusual or lethargic locational patterns.[186] On a

---

expressly offered the right to object free of charge to such disclosures or uses'; Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000, 1–88.

173 UN Global Pulse, *supra* nt. 20.

174 WEF and Kearney, *supra* nt. 38.

175 *Ibid.,* noting a lack of and increasing need for a workable taxonomy.

176 *Ibid*.

177 *Ibid*.

178 Mueller, P. R., Comment, "Every Time You Break, Every Time You Make—I'll Be Watching You: Protecting Driver Privacy in Event Data Recorder Information", *Wisconsin Law Review*, 2006, 135–189.

179 WEF and Kearney, *supra* nt. 38.

180 *Ibid*.

181 *Ibid*.

182 *Ibid*.

183 *Ibid*.

184 MIT Technology Review, Talbot, D., *Big Data from Cheap Phones*, 23 April 2013, available online at <technologyreview.com/featuredstory/513721/big-data-from-cheap-phones/> (accessed 20 October 2014).

185 The Wall Street Journal, Hotz, R. L., *The Really Smart Phone*, 23 April 2011, available online at <online.wsj.com/news/articles/SB10001424052748704547604576263261679848814> (accessed 20 October 2014).

186 Diabetes Health, Silberstein, N., *Mobile Technology and Blood Glucose Monitoring, Diabetes Health*, 24 June 2007, available online at <diabeteshealth.com/read/2007/06/24/5286/mobile-technology-and-blood-glucose-monitoring/> (accessed 20 October 2014); The New York Times, Wayner, P., *Monitoring Your Health with Mobile Devices*, 22 February 2012, available online at <nytimes.com/2012/02/23/technology/personaltech/monitoring-your-health-with-mobile-devices.html?_r=0> (accessed 20 October 2014).

macro level, large-scale locational data reveal where populations go in the midst of a pandemic, even suggesting 'early warning systems' that far outpace traditional warning methods.[187] Researchers at IBM analysed data and proscribed more efficient bus routes based on people's movements derived from millions of cell phone users in the Ivory Coast.[188]

When sharing location data, mobile companies often aver that they anonymise data before transferring it, either for profit or charitable purposes.[189] Blacking out user names and phone numbers before selling locational data however, fails to satisfy privacy advocates. MIT researchers Cesar A. Hidalgo and Yves-Alexandre de Montjoye demonstrated that four data points about a phone's location can usually identify the user.[190] In fact, with a little more data, researchers divined information about a person's "future" location. One study predicted a person's approximate location up to eighty weeks in the future—with 80% accuracy.[191]

Mobile phone locational data is only one example. Passively generated data and the concomitant dilution of the individual's ownership thereof is accelerating.[192] Individuals exude "data exhaust": actions, choices, locations, and preferences as they go about their daily lives. Proliferating sensors digitally track, store, and communicate these actions to the Internet.[193] 'From 2012 to 2017, machine-to-machine traffic will grow an estimated 24 times to 6 x 1017 bytes per month'.[194] Cisco projects fifty billion devices will connect to the Internet by 2020,[195] but other valid estimates reach up to 200 billion by the same year.[196] Even today, more things are connected to the Internet than there are people in the world.[197] Like locational data from mobile phones, the data generated in an "Internet of Things", will be largely passive.

---

187 Mayer-Schonberger and Cukier, *supra* nt. 13.

188 Talbot, *supra* nt. 90.

189 MIT Technology Review, Leber, J., *How Wireless Carriers are Monetizing Your Movements*, 12 April 2013, available online at <technologyreview.com/news/513016/how-wireless-carriers-are-monetizing-your-movements/> (accessed 20 October 2014).

190 MIT News, Hardesty, L., *How hard is it to 'de-anonymize' cellphone data?,* 27 March 2013, available online at <newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>; see also de Montjoye, Y. A., *Projects*, available online at demontjoye.com/projects.html (accessed 20 October 2014).

191 Tucker, *supra* nt. 22.

192 WEF and Kearney, *supra* nt. 38.

193 Mundie, *supra* nt. 151.

194 WEF and Kearney, *supra* nt. 38, 16.

195 Ericsson, *Ericsson White Paper: More than 50 Billion Connected Devices* , February 2011, available online at <akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices.pdf> (accessed 20 October 2014).

196 Bajarin, *supra* nt. 1.

197 *Ibid*.

III.3. Internet of Things

The Internet of Things avoids precise definition.[198] In layman's terms, everyday devices—objects—talk to one another online. Connecting objects to a mobile or wired network enables the object to send and receive data automatically without human intervention.[199] Outfitting innumerable objects with tiny identifying and transmitting technology could be radically transforming. One commentator, perhaps dramatically, avers that 'no technology breakthrough since the introduction of telephone networks themselves, with the possible exception of the Internet itself, puts as massive and fundamental changes on the table as the Internet of Things'.[200]

With billions of passive sensors communicating to the Internet already,[201] the Internet of Things is more science than science fiction. From home to the car to work, the Internet of Things captures passive data about individuals and transmits them to the Internet.

III.3.1. Internet of Things at Home

Consider smart meters. Meaningful efficiencies attend electronic sensors that identify, analyse and communicate electricity use from an individual residence to a utility company.[202] Instead of employing workers to walk neighbourhoods reading each resident's meter every six months and then estimating monthly usage from prior history, smart meters provide real time granular data.[203] As of 2012, approximately thirty-six million smart meters record and transmit energy use in the US,[204] and over 200 million smart meters will be installed in the EU by 2020.[205]

A recent eighty-five-page White House report notes the benefits of smart meters, but also admits that they can 'show when you move about your house'.[206] The Report cites

---

198 Dr.Vermesan, O., Dr. Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Dr. Bassi, A., Jubert, I. S., Dr. Mazura, M., Dr. Harrison, M., Dr. Eisenhauee, M., Dr. Doody, P., "Internet of Things Strategic Research Roadmap", *in*: Vermesan, O. and Friess, P., eds., *Internet of Things—Global Technological and Societal Trends*, River Publishers, Denmark, 2011, 9–52, 10, defining the Internet of Things as 'an integrated part of Future Internet including existing and evolving Internet and network developments and could be conceptually defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network'.

199 The Value of Our Digital Identity, *supra* nt. 27.

200 IT Business Edge, Weinschenk, C., *Impossible to Overestimate Impact of the Internet of Things*, 30 June 2014, available online at <itbusinessedge.com/blogs/data-and-telecom/impossible-to-overestimate-impact-of-the-internet-of-things.html> (accessed 20 October 2014); see also RFID Journal, Ashton, K., *That Internet of Things' Thing*, 22 July 2009, available online at <rfidjournal.com/articles/view?4986> (accessed 20 October 2014), 'The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so'.

201 Bajarin, *supra* nt. 1.

202 Balough, C. D., "Privacy Implications of Smart Meters", *Chicago Kent Law Review*, vol. 86, ed. 1, 2011, 161–191; Stern, S. M., "Smart-Grid and the Psychology of Environmental Behavior Change", *Chicago Kent Law Review*, vol. 86, ed. 1, 2011, 139–160.

203 *Ibid*.

204 US Energy Information Administration, *Smart Meter Deployments Continue to Rise*, 1 November 2012, available online at <eia.gov/todayinenergy/detail.cfm?id=8590> (accessed 20 October 2014).

205 Navigant Research, *Smart Meters in Europe*, available online at <navigantresearch.com/research/smart-meters-in-europe> (accessed on 20 October 2014).

206 Executive Office of the President, The White House Report, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, available online at

Cornell Professor, Stephen Wicker, who is a bit more specific, noting that electrical devices have unique signatures, and some metering can 'distinguish the microwave from refrigerator, or even the light bulb in the bathroom from the light bulb in the dining room'.[207] Instead of simply knowing a resident's approximate monthly electricity use, smart meters reveal when a person is home, cooking, showering, watching television or on vacation.[208] The information can be used to infer whether the resident is wealthy, clean, healthy or sleep deprived.[209] One illustrative study showed with 96% accuracy that the exact television show or movie being watched could be divined solely from the electrical signal coming from an individual's home.[210]

In addition to smart meters, "smart homes" infuse sensors throughout the home to track resident behaviour and alter home conditions autonomously.[211] Google recently paid USD3.2 billion for Nest, a company that sells thermostats that track residential behaviour in order to adjust home temperature more efficiently.[212] Why spend so much for a self-adjusting thermostat? Nest's value resides in the connections it generates among its devices.[213] In other words, Nest's thermostat does more than cool a room when the resident returns home from work. 'Over time, as the Nest Learning Thermostat uses its sensors to train itself according to your comings and goings, the entire network of Nests in homes across the country becomes smarter'.[214] It is not the thermostat itself that boosts Nest's value, but the interconnectedness of all those thermostats. As the devices talk to each other, they construct an aggregate picture of human behaviour, and predict or anticipate what users want before they know it.[215]

Other home apps or devices use sensors to detect water leaks, open doors, energy use and home security.[216] Sensors can send a text message alerting you that the garage door is open, the bathroom light is on, or that the plants need watering.[217] While the home

---

<whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf> (accessed 20 October 2014).

207 Cornell University, Wicker, S., and Thomas, R., *A Privacy-Aware Architecture For Demand Response Systems*, Proceedings of the 44th Hawaiian Conference on System Science (HICSS-44), Kauai, Hawaii, January 2011 available online at <wisl.ece.cornell.edu/wicker/SWicker_RThomas_HICSS.pdf> (accessed 20 October 2014); see also Computerworld, Thibodeau, P., *The Internet of Things could encroach on personal privacy*, 3 May 2014, available online at <computerworld.com/article/2488949/emerging-technology/the-internet-of-things-could-encroach-on-personal-privacy.html> (accessed 20 October 2014).

208 *Ibid*.

209 *Ibid*.

210 Enev, M. *et al.*, "Inferring TV Content from Electrical Noise", 2011, available online at <miro.enev.us/papers/EMI_CCS_2011.pdf> (accessed 25 November 2014); see also Naked Security, Wisniewski, C., *Smart meter hacking can disclose which TV shows and movies you watch*, 8 January 2012, available online at <nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/> (accessed 20 October 2014).

211 Balough, *supra* nt. 202.

212 Wired, Wohlsen, M., *What Google Really Gets Out of Buying Nest for $3.2 Billion*, 14 January 2014, available online at <wired.com/2014/01/googles-3-billion-nest-buy-finally-make-internet-things-real-us/> (accessed 20 October 2014).

213 *Ibid*.

214 *Ibid*.

215 *Ibid*.

216 Postscapes, Rushing, K., *Wireless Home Sensor Systems*, available online at <postscapes.com/home-wireless-sensor-systems> (accessed 9 December 2014).

217 HGTV, *11 Smart Apps for Your Home*, available online at <hgtv.com/remodel/mechanical-systems/11-smart-apps-for-your-home> (accessed 9 December 2014).

applications of the Internet of Things have been growing and evolving, the user privacy implications have been largely ignored.

III.3.2. Internet of Things in the Car

Walk from the house to the car and the Internet of Things will follow. Toll tags, for example, include radio-frequency identification (RFID) technology that communicates with receptors at toll gantries in order to detect and record when a car passes.[218] While toll agencies routinely protect billing information associated with toll tags, few policies, if any, protect the personal information gathered. Indeed, in New York, toll tags reveal the driver's location in many part of the city regardless of toll gantries. Unbeknownst to users, New York traffic officials designed other uses for toll tags by erecting receptors throughout the city in order to better understand traffic flow in real time.[219] While improving traffic in New York seems innocuous (if unlikely) the technology allows constant automobile tracking without the driver's awareness or any assurance that the information will not be used or sold for other purposes.[220]

Don't use toll tags? License plate readers are proliferating among both private[221] and public organisations.[222] License plate readers capture license plate numbers, as well as the date, time and location of every scan.[223] Policing agencies across the United States collect and often pool this information, retaining the data for unspecified terms.[224] One civil rights group conducted a lengthy investigation among thirty-eight states and 600 local police departments before concluding that 'the documents paint a startling picture of a technology deployed with too few rules that is becoming a tool for mass routine location tracking and surveillance'.[225]

In one Texas city, police scanned an average of 14,547 license plates per day, and retained the information on almost two million license plates in its database.[226] Private entities also track automobiles using license plate readers and then sell the information to third parties, like repossession debt collectors and insurance companies.[227] Two private companies in the US recently collected 'tens of millions of pieces of geo-located information from thousands of license plate readers, mounted on tow trucks, mall

---

218 Forbes, Hill, K., *E-ZPasses Get Read All Over New York (Not Just At Toll Booths),* 12 September 2013, available online at <forbes.com/sites/kashmirhill/2013/09/12/e-zpasses-get-read-all-over-new-york-not-just-at-toll-booths/> (accessed 20 October 2014).

219 *Ibid.*

220 *Ibid.*

221 NBC News, Aegerter, G., *Licence Plate Data Not Just for Cops: Private Companies Are Tracking Your Car*, 1919 July 2013, available online at <nbcnews.com/news/other/license-plate-data-not-just-cops-private-companies-are-tracking-f6C10684677> (accessed 20 october 2014).

222 Center for Investigative Reporting, Winston, A., *Plans to Expand Scope of License-Plate Readers Alarm Privacy Advocates*, 17 June 2014, available online at <cironline.org/reports/plans-expand-scope-license-plate-readers-alarm-privacy-advocates-6451> (accessed 20 October 2014).

223 Merola, L. M. and Lum, C., "Emerging Surveillance Technologies: Privacy and the Case of License Plate Recognition (LPR) Technology", *Judicature*, vol. 96, 2012, 119–126.

224 American Civil Liberties Union, *You Are Being Tracked: How License Plate Readers Are Being Used to Record American's Movements*, 17 July 2013, available online at <aclu.org/alpr> (accessed 20 October 2014).

225 *Ibid*.

226 *Ibid*.

227 NBC News, Aegerter, G., *Licence Plate Data Not Just for Cops: Private Companies Are Tracking Your Car*, 19 July 2013, available online at <nbcnews.com/news/other/license-plate-data-not-just-cops-private-companies-are-tracking-f6C10684677> (accessed 20 October 2014).

security vehicles, police cars, at the entrances to store parking lots, on toll booths or along city streets and highways'.[228]

Combined with other data about an individual, license plate tracking becomes especially troubling because it reveals an impressive depth of field.[229] One California maker of license plate readers plans to fuse locational information from license plate trackers with public record data and eventually facial recognition technology by comparing real time snapshots with photographs from the local department of motor vehicles database.[230]

In contrast to toll tags and license plate readers, several devices *inside* the car collect and disseminate data. "Black boxes" or event data recorders log and retain driving data in most cars sold in the US in the past twenty years.[231] These sensors typically archive speed, revolutions per minute, brake usage, and the sequence of speed and braking immediately before and after a wreck or sudden stop.[232] Insurance companies urge customers to install similar devices that monitor and report speed, miles travelled, acceleration and braking.[233] Presumably, a continuous real-time data feed from thousands of automobiles allows underwriters to better assess risk.[234]

Of course, most cars carry their own GPS systems, with newer cars boasting more sensors and Internet connections, allowing for services ranging from voice activated restaurant recommendations nearby,[235] to automated searches for parking spots across twenty European countries.[236] A majority of industry experts project that connectivity will soon be the principle factor in car purchasing.[237] The consistent and unanswered question remains: How will this data be stored, transferred and used?

III.3.3. The Internet of Things at Work

The Internet of Things does not disappear when leaving the car and entering the workplace. Apart from ubiquitous upper corner video cameras, new data devices in the workplace capture and communicate employees' location, duration of breaks, productivity in completing discrete tasks and more.[238] Identification badges loaded with sensors measure employees' tone of voice, rapidity of speech and social interactions.[239]

---

228 *Ibid*.

229 *Ibid*.

230 Center for Investigative Reporting, Winston, A., *Plans to Expand Scope of License-Plate Readers Alarm Privacy Advocates*, 17 June 2014, available online at <cironline.org/reports/plans-expand-scope-license-plate-readers-alarm-privacy-advocates-6451> (accessed 20 October 2014).

231 National Highway Traffic Safety Administration, "Event Data Recorders", *Federal Register*, vol. 69, 14 June 2014, 32932–32954, 32932–32933.

232 Mueller, *supra* nt. 179.

233 *Id.*, 155–160.

234 *Ibid*.

235 See Ford Webpage, *Explore Navigation by Voice*, available online at <support.ford.com/sync-technology/navigation-by-voice-sync-myford-touch> (accessed 20 October 2014).

236 See Parkopedia Webpage, *Parkopedia*, available online at <en.parkopedia.com/> (accessed 20 October 2014).

237 Forbes, Clark, T., *At Mobile World Congress, A Connected Future Becomes Reality*, 27 February 2014, available online at <forbes.com/sites/sap/2014/02/27/at-mobile-world-congress-a-connected-future-becomes-reality/> (accessed 20 October 2014).

238 MIT Technology Review, Waber, B., *Augmenting Social Reality in the Workplace*, 15 May 2013, available online at <technologyreview.com/news/514371/augmenting-social-reality-in-the-workplace/> (accessed at 20 October 2014).

239 *Ibid*; Wall Street Journal, Wilson, J. H., *Wearable Gadgets Transform How Companies Do Business*, 20 October 2013, available online at <online.wsj.com/articles/wearable-gadgets-transform-how-companies-do-business-1382128410?tesla=y> (accessed 25 November 2014).

One company found that more socially engaged employees performed better,[240] leading a CEO to claim that he can predict 'from a worker's patterns of movement whether that employee is likely to leave the company, or score a promotion'.[241]

Another company seeks to use data sensors and analytics to augment social interactions in the workplace.[242] Analytical software set to optimise productivity determines which employees should be talking or socialising with certain other employees.[243] To repeat, software—in the interest of productivity—determines which employees should be interacting.[244] Actual workplace walls, coffee machine locations and other commons areas robotically move based on this algorithm to encourage specific employees to interact at specific times.[245] 'Unlike augmented reality, which layers information on top of video or your field of view to provide extra information about the world, augmented social reality is about systems that change reality…'.[246]

All of these sensors—at home, in the car, or at work—generate terabytes of data, much of it personal and most of it unregulated. Libraries affix RFIDs to every book in their collections.[247] Dentists graft sensors into toothbrushes that measure how you brush, identify problem areas, and send the bad news to the cloud for virtual check-ups.[248] Thousands of other examples range from tilt sensors in beer mugs that record how much someone consumes[249] to ingestible pharmaceuticals that measure and transmit internal bodily functioning.[250]

We generate much of this passive data simply by moving from one place to another; it is nearly impossible not to emit data exhaust. Everyday objects equipped with sensors that communicate with the Internet already exist and more are on the way.[251] Over 200 billion worldwide are expected by 2020.[252] For the cost of a few pennies each, RFIDs have the capability to track just about anything.[253] It is entirely feasible, if not likely, that most retail products will soon carry RFID tags that transmit data to a computer when it

---

240 *Ibid.*

241 Wall Street Journal, Silverman, R. E., *Tracking Sensors Invade the Workplace*, 7 March 2013, available online at <online.wsj.com/articles/SB10001424127887324034804578344303429080678> (accessed 25 November 2014).

242 Waber, *supra* nt. 238.

243 *Ibid*.

244 *Ibid*.

245 *Ibid*.

246 *Ibid.*

247 Molnar and Wanger, *supra* nt. 3, the study suggests that readers set up at airport security could identify those with "hotlisted" books and detain them for additional screening.

248 Forbes, Clark, T., *At Mobile World Congress, A Connecctd Future Becomes Reality*, 27 February 2014, available online at <forbes.com/sites/sap/2014/02/27/at-mobile-world-congress-a-connected-future-becomes-reality/> (accessed 20 October 2014).

249 Wired, Thompson, C., *No Longer Vaporware: The Internet of Things is Finally Talking*, 6 December 2012, available online at <wired.com/2012/12/20-12-st_thompson/> (accessed 20 October 2014).

250 See e.g., Proteus Digital Health, *Digital Health Feedback System*, available online at <proteus.com/technology/digital-health-feedback-system/> (accessed 20 October 2014).

251 WEF and Kearney, *supra* nt. 38.

252 Bajarin, *supra* nt. 1.

253 Schmidt, J. M., "RFID and Privacy: Living in Perfect Harmony", *Rutgers Computer and Technology Law Journal*, vol. 34, 2007, 247–272, 250–252.

is within twenty feet of a reader.[254] 'Pretty much everything you can imagine will wake up.'[255]

Given the expansion of sensors and the emergence of the Internet of Things, it is becoming increasingly unlikely that a person could know precisely how much of their data is captured, who controls it and for what purpose.

IV. Privacy Regulation Through Risk Management

The leading law on privacy, the EU's 1995 Directive, attempts to protect a user's personal information in a number of ways. Primarily, the law requires those who process personal information to give notice to the user and then allow the user to opt out.[256] The user must consent, in other words, before an entity can collect personal data.[257] The law also allows users to access and correct their personal data after it has been collected by another.[258]

Apart from the problematic and overbroad concept of "personal information",[259] the law fails to account for the Internet of Things. It fails to countenance the proliferation of passive data collection, and instead relies on the faulty premise that users actively volunteer all personal information.[260] Notice and consent obligations, like those in the Directive, apply poorly to passive data collection.[261]

How do businesses and governments issue notice and obtain consent from every person strolling on the sidewalk, whose images are captured by rooftop cameras? Must toll tag and license plate readers notify and obtain consent before every scan? Can residents withhold their consent to data gathering when a municipal government requires them to use smart meters? For those municipalities that do allow residents to opt-out of smart metering, does the notice provide clarity with regard to the amount of data collected and if so, can a resident access and correct that data? (*I was using the microwave, not the shower at 10:50pm on 11 August 2014.*) Does the notice include notice of potential or future uses of such data, including sale or transfer to third parties?

Requiring employers to provide notice and obtain consent before monitoring employee location, productivity and behavior poses similar difficulties. Even if a single global consent sufficed rather than requiring employers to obtain consent each time an employee's behavior is monitored, that consent is often illusory; no consent, no job.[262] Even in the home, users who purchase and install a Nest thermostat are likely consenting

---

254 *Ibid*; Kobelev, O., "Recent Development, Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response", *North Carolina Journal of Law & Technology*, vol. 6, ed. 2, 2005, 325–342.

255 Cisco, *What is the Internet of Everything*, available online at <cisco.com/web/tomorrow-starts-here/ioe/> (accessed 25 November 2014).

256 Directive 95/46/EC, *supra* nt. 9, Article 14(b), requiring that individuals 'be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses'; Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000, 1–88.

257 *Ibid.*

258 *Ibid.*

259 Taylor, *supra* nt. 100.

260 WEF and Kearney, *supra* nt. 38, 16.

261 *Ibid.*

262 Levin, A., "Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada", *Canadian Journal of Law and Society*, vol. 22 ed. 2, 2007, 197–230; Willborn, S. L., "Consenting Employees: Workplace Privacy and the Role of Consent", *Louisiana Law Review*, vol. 66, ed. 4, 2006, 975–1008.

to the use of their personal information in order to optimise the home's temperature.[263] But does this consent extend to sharing that information with countless other automated thermostats and using aggregated information to predict future behavior? Does their consent cover neighbours or other invitees to the home?

One report from the 2014 World Economic Forum put it this way: 'With an increasing proportion of personal data now being passively collected by sensors or synthetically generated by algorithms, engaging individuals for consent to use data they know nothing about (and for purposes which are yet to be defined) remains problematic.'[264] Notice, consent, access and correction, while arguably useful tools regulating a user's voluntary divulgence of personal information, fall short when personal data is passively obtained. Current privacy laws miscarry when data 'originates at a distance from the immediate perception of individuals and where consent, participation and awareness are seldom feasible'.[265]

Instead of a broad privacy law that declares all personal data to be protected and that requires notice and consent before data collection, privacy laws should narrowly target specific harms that attend specific informational privacy violations. Regulating the *use* of sensitive data as it relates to particular risks or harms better comports with consumer law generally and permits the needed adaptability to reflect context and changing technology.[266]

This is not a novel idea.[267] Some in the privacy community liken this proposed regulatory approach to the field of risk management.[268] Calibrating the risk or the harm from the individual's viewpoint in using data in a particular way reveals the value of that data and allows local regulatory regimes to adopt protective policies incrementally.[269] It requires a normative taxonomy regarding data usage.[270] How is particular data used in a particular context? Sector or Industry-specific uses may provide a starting point; educational uses differ from healthcare uses or advertisement uses.

Within a given context or sector, a particular use would include parameters on who is authorised to process the data and for what purposes. Depending on context, user preferences could be factored in. Identifying and defining diverse data contexts and uses, and identifying the attendant risks or harms from the user's viewpoint are critical to successful implementation of contextual and harm-based personal data regulation.

License plate readers, for example, are sporadically and sparsely regulated throughout the United States.[271] Identifying the benefits of license plate readers, the privacy risks or harms from the individual's viewpoint, and the various uses that gleaned data may have, strengthens the likelihood of creating concrete policy and pragmatic regulation—much

---

263 Nest, *Terms of Service*, available online at <nest.com/legal/terms-of-service/> (accessed 20 October 2014).

264 WEF and Kearney, *supra* nt. 38, 10.

265 *Ibid.*

266 Spina, A., "Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?", *European Journal of Risk Regulation,* vol. 5, ed. 2, 2014, 248–252.

267 *Ibid*; Centre for Information Privacy Leadership, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, 19 June 2014, available online at <hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf> (accessed 20 October 2014) (Post Paris Risk Paper).

268 Centre for Information Privacy Leadership, *Privacy Risk Framework and Risk-based Approach to Privacy*, 2014, available online at <informationpolicycentre.com/privacy_risk_framework/>; see also Post Paris Risk Paper, *supra* nt. 267.

269 *Ibid*; Spina, *supra* nt. 266.

270 WEF and Kearney, *supra* nt. 38.

271 American Civil Liberties Union, *supra* nt. 224.

more so than a global prohibition on collecting almost all personal information unless each individual is given notice and then consents. Policymakers might recognise the benefit to law enforcement and allow license plate readers for the specific purpose of pursuing certain criminal investigations. The harms or risks to individuals, however, might lead policymakers to outlaw storage of license plate data about innocent people as well as sharing that data with third parties. By addressing data collection from the individual's viewpoint, institutions can better identify privacy risks and create usage policies to minimise the same.[272]

Institutions gathering or using sensitive data can prioritise risk and use by asking: What is the intended use? What risks to the individual attend that use and how likely is it for that harm to occur? How severe is the harm: loss of property, physical injury or reputational damage?[273] Prioritisation based on seriousness or likelihood of harm borrows from traditional risk management protocols and allows policymaking that is tailored to context. 'Risk management can be applied across the data value chain to more granularly access systemic reliability, codes of conduct and legal compliance.'[274]

Of course, this approach is not a panacea. Different individuals perceive privacy harms differently. Many have suggested that generally, Americans are far less concerned about certain privacy matters than Europeans.[275] Moreover, individuals, regardless of residence, may have dramatically different privacy sensibilities. To one person, cookies that remember past Internet purchases are harmless; to another they are abhorrent. But the law has long accepted and regulated diverse individual perceptions of harm and risk.[276]

Effective regulation that protects individual privacy while facilitating innovation is a Gordian knot,[277] especially in light of the deluge of easily accessible data combined with rapidly changing technology. The proliferation of data, elaborate analytical capabilities and borderless flow of digital information befog regulatory efforts. Compounding the problem, data increasingly originates passively from sensors and analytic compilations, rendering individuals less aware and more distant from decisions regarding the use of their data.

For these reasons, and others not mentioned, global privacy regulation will remain formidable. But the bedeviling attributes plaguing data privacy also suggest that omnibus privacy laws like the Directive undermine privacy as much as protect it. Laws that provide blanket prohibitions and that hinge on an expansive understanding of personal information and that call for individuals' notice and consent cannot be fairly applied or enforced. A risk of harm-based legal framework that turns on the use of information contextualises potential privacy violations and allows institutions and governments to customise policies relevant to the risk of harm.

---

272 Post Paris Risk Paper, *supra* nt. 267.

273 *Ibid*.

274 WEF and Kearney, *supra* nt. 38, 18.

275 See e.g., Whitman, J. Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *The Yale Law Journal*, vol. 113, 2004, 1151–1221, 1194; Walker, R. K., "The Right to Be Forgotten", *Hastings Law Journal*, vol. 64, 2012, 257–286.

276 Spina, *supra* nt. 266.

277 Encyclopedia Britannica, *Gordian Knot*, available online at <britannica.com/EBchecked/topic/239059/Gordian-knot> (accessed 25 November 2014).

V. Conclusion

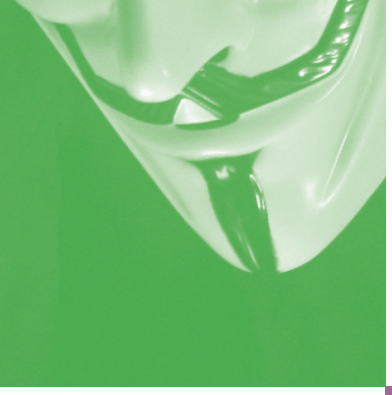
Legacy privacy laws, like the EU Directive, seek to protect privacy in the Age of Information. They are failing. To some degree, they undermine privacy by restricting all processing of personal information—even processing that would ensure that data remains secure and therefore private. They cast a wide net; the laws include almost any data pertaining to a person. With burgeoning de-anonymising algorithms, efforts to scrub identifying data prove fruitless, resulting in an ever-expanding reach. As a result, the Directive and laws like it capture a great ocean of data processing, which foments uncertainty and uneven enforcement, rather than harmonising data processing regulation. The laws' laudable goal in principle, is reduced to platitude and bureaucracy in practice.

The Internet of Things sharpens this dysfunction. The Directive rests on the faltering presumption that individuals voluntarily divulge personal information, when the growing trend indicates a wide lacuna between user awareness and data collection. Users do not voluntarily post GPS locational data every few seconds or record and transmit automobile acceleration and braking events.

Privacy laws that turn on personal information and that require notice and consent before data collection poorly reflect the technological landscape and remain impractical at best. Privacy laws should focus on data use, not collection. Privacy laws should identify and address the specific harm or risk associated with the use of sensitive data in particular contexts. Among the privacy community, this approach is likened to the field of risk management. It allows contextualisation among privacy laws and encourages incremental and adaptable regulation based on specific risks associated with potential misuse of sensitive data.

Informational privacy is ominously fleeting. We have already passed the point and missed the opportunity of effectively regulating the collection of personal data. Rather than persist in vain to try regulating the collection of personal data, policymakers should consider regulating its use based on risk of harm.

*



GRONINGEN **JOURNAL OF INTERNATIONAL LAW**

CRAFTING HORIZONS

ISSN 2352-2674

PHOTOGRAPHY: BRIAN KLUG