Groningen Journal of International Law, vol 2(2): Privacy in International Law

The Internationalisation of Information Privacy: Towards a Common Protection

Bo Zhao*

DOI: 10.21827/5a86a803f1c1a

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 business level where more companies adjust business strategies according to collected

---

[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.

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 exemplifying the strong need for "sharing" and "being connected" is a Russian soldier's

---

[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.

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.

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.

---

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.

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

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

---

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

strengthening data protection with the proposed new data protection package.[67]

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

---

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

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]

*

www.grojil.org

---

[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).