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

Bridging the gap between individual privacy and public security

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

DOI: 10.21827/5a86a80e3f56e

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 Dateniüberwachung 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.