Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century

Klitou, D.G.

2 Privacy, liberty & security

2.1 CHAPTER INTRODUCTION

Privacy, liberty and security are important, inter-related concepts that have been debated for centuries.

Section 2.2 outlines the concept of privacy. Section 2.3 provides an overview of the international legal instruments that stipulate the right to privacy. Section 2.4 explains briefly the merits of privacy. Section 2.5 outlines the concept of liberty. Section 2.6 clarifies the relationship between privacy and liberty. Section 2.7 outlines the concept of security. Section 2.8 concludes the chapter with an explanation of the interlinkages between privacy, liberty and security.

2.2 THE CONCEPT OF PRIVACY

Again, it is not the intention of this dissertation to attempt to formulate a comprehensive, specific and widely agreed upon definition of privacy. Instead, the dissertation focuses on assessing the existing legal frameworks, in light of the latest PITs, and on presenting practical, legal and technical measures to safeguard privacy/liberty. Moreover, this dissertation does not focus on conclusively defining the concept of privacy, since such an endeavor is not feasible for a dissertation alone, due to the vast array of different theories and conceptualizations of privacy and conflicting opinions. As Wacks notably once argued, "the long search for a definition of 'privacy' has produced a continuing debate that is often sterile and, ultimately, futile" (1980, p. 10).[13] Even the ECtHR, as Taylor points out, "has never sought to give a conclusive definition of privacy, considering it neither necessary nor desirable" (2002a, p.76). Other legal scholars (e.g. Solove, 2006) have also observed the difficulty and ineffectiveness of trying to conclu-

[13] For further discussion, see Taylor, Nick. *State Surveillance and the Right to Privacy* (Surveillance & Society 1, 2002a), pp. 66-85.

sively and comprehensively define privacy. However, it did not take long to discover that privacy is so difficult to define. Sir James Fitzjames Stephen, more than a century ago, argued "[t]o define the province of privacy distinctly is impossible, but it can be described in general terms" (1873, p. 160).

It may be fair to presume that this enduring futility or difficulty of reaching a comprehensive and determined consensus on the definition of privacy (i.e. what fully constitutes privacy, what constitutes a privacy violation, what merits privacy protection) is the result of the concept's "inherent flexibility"[14] and the significant differences of opinion among legal practitioners/legal scholars and between different generations. For instance, Generation X may overall have a different opinion about privacy and its importance/value than Generation Y (or the "Millennial Generation"). Moreover, the need to take into consideration the current/changing social norms/values, public opinions, ideological trends, available technologies, political circumstances and overall state of affairs (e.g. an extraordinarily high violent crime rate or the aftermath of a terrorist attack) make it even more difficult to broadly/comprehensively define privacy in a fixed and definitive way. The concept of privacy and the belief in its importance/value may also differ among people based on their personalities, personal experiences, interests and more particularly on their occupation and position/role within society. The escalating advancement, deployment and use of PITs have also added to this uncertainty and the difficulty in defining privacy (see section 4.2 for the dissertation's definition of PITs). For example, it may be especially more difficult to define privacy in a high-tech "surveillance society" or within a "ubiquitous information society". Therefore, it should come as no surprise that a consensus on the definition of privacy has yet to be achieved, and the notion of doing so will only become more complicated in the future as technologies continuously advance and social values potentially change. Nevertheless, *the underlying concept of privacy*, which serves as the basis of this dissertation, should be somewhat outlined.

At first, the right to privacy was largely viewed, in US courts, as a defense against any "unreasonable" physical intrusion upon one's private home, private papers, personal belongings and person (i.e. body), strictly in accordance with the Fourth Amendment of the US Constitution. The focal point of the concept of privacy and its legal interpretations, however, has gradually evolved over time, beyond those domains, as modern technology and society has evolved. For starters, as widely recognized, Warren and Brandeis (1890) brought a new focus on the autonomy and seclusion components of privacy, in the wake of the increase in newspapers and photographs, made possible

[14] Feldman, Noah. "Strip-Search Case Reflects Death of American Privacy" (Bloomberg, 9 April 2012), available at: http://www.bloomberg.com/news/2012-04-08/strip-search-case-reflects-death-of-american-privacy.html

by printing technologies and the first cameras (Schermer, 2007), and famously characterized privacy as the right "to be let alone" (Warren and Brandeis, 1890, p. 193). With the rapidly growing use of telephones, the focus of privacy evolved to the privacy of telecommunications. The gradual increase in the use of information technologies/electronic data systems led to the focus on the privacy of personal data stored on computer databases – 'information privacy'.[15] Accordingly, Westin notably defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated" (Westin, 1967, p. 7). As questions arose on the morality and legality of abortion and the means employed, the focus of privacy further evolved to personal autonomy/self-determination and the right of individuals to make decisions concerning their own bodies and/or domestic matters. As the advancement, deployment and use of public surveillance CCTV cameras has rapidly increased, and the development of other technologies capable of mass surveillance advances, the right to be left alone has been re-emphasized. The advancement and use of location-tracking devices, location-based services and mobile phones capable of being tracked has led to the focus on 'location privacy' and the privacy of location information. It has also re-initiated a debate on the level of privacy that may (or may not) exist out in public. As the use of e-mail, online social networking (Facebook, etc.), micro-blogging (i.e. Twitter) and e-commerce websites (Amazon, eBay, etc.) continue to increase, the focus of privacy has also swiftly evolved to further address the confidentiality of online (and related offline) activities and initiated the debate on how the 'right to be left alone' could be extended to the information society. As electronic voting machines surfaced and their deployment and use during elections increased, and the potential for the implementation of Internet voting also increases, privacy has also re-focused on the importance of the sanctity of the vote in a democratic society. As electronic health records rapidly increase, the focus of privacy further emphasized the confidentiality of personal medical data. As neurotechnology advances and its applications increase, a new focus of privacy will likely evolve to address the privacy of the mind/brain.[16] As the immense potential of DNA analysis emerged and the use of biometric data increased, the focus of privacy has evolved even further to the privacy of the body (or bodily/corporeal privacy). However, while the concept and focus (i.e. focal point) of privacy is continuously evolving and varies from time to time as technology and society

[15] For the purposes of this dissertation, 'information privacy' is synonymous with 'data protection'.

[16] see "Clive Thompson on Why the Next Civil Rights Battle Will Be Over the Mind" (Wired, 24 March, 2008), available at: http://www.wired.com/techbiz/people/magazine/16-04/st_thompson

evolves, what was previously considered applicable continues to remain relevant, since all of these technologies are still heavily in use.

Privacy, therefore, is not just simply an issue concerning the inviolability of one's private home, private papers, etc. or what is done with one's personal data.[17] For the *underlying and particular purposes of this dissertation*, an understanding of privacy includes the inviolability of a person's mind and body (unless lawfully authorized), the protection of the confidentiality of personal data, the 'right to be left alone', the 'reasonable' confidentiality of communications between two or more people no matter where, how and in what form they occur, and the freedom from undue, unlawful or unreasonable surveillance, whether in public or private places.[18]

The 'right to be left alone' is associated with the freedom from unreasonable, unlawful or disproportionate surveillance and also the right to be free from unnecessary or excessive disturbance, which can interfere with a person's life. This component of privacy, for example, has likely supported the establishment of the National Do Not Call Registry (McClurg, 1995) and the adoption of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 in the US, which regulates spam e-mail, and in the EU the relevant provisions of Directive 2002/58/EC, which prohibits unsolicited communications in the form of automatic calls or e-mails. The right to privacy and/or the right to be left alone also supported the creation of anti-stalking laws (McClurg, 1995).

Based on Article 2 of EU Directive 95/46/EC, personal data (or personal information) is "any information relating to an identified or identifiable natural person ('data subject')". As Article 2 (a) states:

> An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity is regarded as information that can be used to directly or indirectly identify an individual.[19]

Personal data normally includes, for instance, a name, address, date of birth, identification number, etc. However, personal information of a far more sensitive character, *for*

---

[17] For further discussion on the scope of privacy, see, e.g., Nissenbaum, Helen. *Privacy as Contextual Integrity* (Washington Law Review, Vol. 79, No. 1, 2004), pp. 101-140.

[18] see *Ibid*.

[19] see Article 2 (a) of Directive 95/46/EC.

the underlying purposes of this dissertation, includes a person's consumer habits, daily movements, private affairs and activities, voting records, conversations, interactions, images, medical history, DNA, and financial data. This list is also certainly not exhaustive.

It is also difficult to comprehensively define a violation of privacy, since there are so many different types of violations. Instead of trying to provide a single meaning to privacy violations, Solove developed a 'taxonomy of privacy', classifying the range of privacy violations within four basic groups: information collection; information processing; information dissemination; and invasion; and 16 subgroups: surveillance; interrogation; aggregation; identification; insecurity; secondary use; exclusion; breach of confidentiality; disclosure; exposure; increased accessibility; blackmail; appropriation; distortion; intrusion; and decisional interference (Solove, 2006, 2008).

In altering the degree, scope and manner in which privacy is or can be violated, the advancement of technology has also made it more difficult to broadly define what activities constitute a violation of privacy (and what activities do not). For the *underlying and specific purposes* of this dissertation, however, a violation of the right to privacy constitutes any of the following: the unauthorized intrusion upon a person's mind or body; the collection and/or disclosure of an individual's personal data without their consent and/or knowledge and/or without warranted justification; the unlawful (or disproportional/disproportionate) manner in which surveillance is conducted; and the disproportionate interference with the 'right to be left alone'.

2.3 PRIVACY AS AN INTERNATIONAL HUMAN RIGHT

Privacy as a fundamental human right is recognized by diverse, international instruments, such as the Universal Declaration of Human Rights (Art. 12), International Covenant on Civil and Political Rights (Art. 17), European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 8), Charter of Fundamental Rights of the European Union (Art. 8), American Convention on Human Rights (Art. 11), United Nations Convention on the Rights of the Child (Art. 16), and the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (Art. 14).

Article 12 of the Universal Declaration of Human Rights (UDHR) declares:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the ICCPR is basically identical to Article 12 of the UDHR.

Article 11 of the American Convention of Human Rights states:

1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks.

Article 16 of the Convention on the Rights of the Child states:

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.

Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families states:

> No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states:

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

Article 7 of the Charter of Fundamental Rights of the European Union provides for the right to privacy, and Article 8 explicitly states:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

2.4 THE MERITS OF PRIVACY

While this dissertation will neither explain or analyze in-depth the merits of privacy, since it focuses instead on regulating the new and specific threats to privacy posed by the latest technologies, those merits should be briefly outlined, in order to highlight why privacy matters and deserves considerable attention, especially as significant ICT industry players are increasingly promoting publicly the contrary perspective.

When comparing each of the international human rights instruments listed above, with the exception of the ECHR, it becomes clear that the right to privacy is explicitly linked with the terms "reputation" and "honor". While the ECHR does not specifically mention the terms in Article 8, the ECtHR has equally associated privacy with honor and reputation on numerous occasions. Thus, as a result, the right to privacy is clearly recognized as a crucial element for realizing personal dignity and self-respect and the respect deserved from others.

The right to privacy can help to foster personal autonomy (see, e.g., Feldman, 1994) and can help enable individuals to take decisions concerning domestic matters free from excessive or undue government interference (see, e.g., Feldman, 2002). However, privacy is more than just a constraint on a prying government or the freedom from excessive scrutiny of private matters; it is also an essential component for developing our own identities, for realizing who we are as individuals, and for developing/maintaining different types of relationships (Warner, 2005). "Without privacy people might feel inhibited from forming close relationships within the family, or outside in social groups" (Taylor, 2002a, p. 82). "It [privacy] allows the social spheres to function and as a result a degree of privacy helps the community to function" (*Ibid*.). In that sense, privacy is essential for individuals to develop their personality, achieve self-realization, and enjoy intimate relationships and social and emotional well-being. Hence, the lack of privacy could lead to the undesirable conformity of behavior and obstruction of individuality or individualism (Schermer, 2007, p. 73).

2.5 THE CONCEPT OF LIBERTY

Liberty has found its contemporary meaning from the thinkers Locke, Fitzjames Stephen, Hume, Hobbes, Rousseau, Mill and Berlin (Schermer, 2007). Berlin (1958) prominently classified liberty into 'positive liberty' and 'negative liberty'. Positive liberty confers a citizen's *freedom to* exercise their civil rights, while negative liberty confers a citizen's *freedom from* undue government interference in the exercise of their civil rights (Schermer, 2007).

For the *underlying purposes of this dissertation*, liberty is simply the collective term for fundamental civil, political and social rights, in addition to physical liberty. Civil and political rights include, for example, the freedom of speech/expression, freedom of assembly, freedom of movement and the right to privacy, all of which are widely accepted to be necessary for the establishment and preservation of a free and democratic society.

2.6 PRIVACY AND LIBERTY

Privacy and liberty are interrelated and should be protected in an integrated and comprehensive manner.[20] As the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) point out, "the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data" (para. 29). Privacy is not an end, but rather a means to an end. Instead, the end is greater liberty. In other words, "[p]rivacy is an enabling right; it creates the foundation for other basic entitlements" (Holtzman, 2006, p. 53). For Gavison (1980), privacy also serves to promote liberty and the benefits of a free and democratic society.

The Canada Supreme Court Justice (retired) Hon. Gérard V. La Forest, in *R. v. Dyment*, prominently judged that "privacy is at the heart of liberty in a modern state" and "[t]he restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state".[21] Westin earlier expressed his belief that "a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies" (Westin, 1967, p. 24). The Closing Communiqué of the 28th International Conference of Data Protection and

---

[20] Hence the reason, for example, why Section 222(a)(5)(A) of the Homeland Security Act requires the DHS Chief Privacy Officer to "coordinate with the Officer for Civil Rights and Civil Liberties to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner" (emphasis added).

[21] *R. v. Dyment* [1988] 2 S.C.R. 417, at 427-8.

Privacy Commissioners (London, 2006) identified that the "protection of citizens' privacy and personal data is vital for any democratic society, on the same level as freedom of the press or the freedom of movement".[22] The Communiqué further added: "Privacy and data protection may, in fact, be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous".[23] As the Madrid Declaration warns, "the failure to safeguard privacy jeopardizes associated freedoms, including freedom of expression, freedom of assembly, freedom of access to information, non-discrimination, and ultimately the stability of constitutional democracies".[24]

Privacy also encourages, to a certain degree, the participation of citizens in the overall democratic process, the exercise of freedom of speech/expression, public discourse and the freedom of movement – all of which are necessary in a democratic and free society. For example, privacy: requires the preservation of secret balloting during an election; rejects the calculated attempt to identify participants at a peaceful protest or to expose the identity of bloggers/writers/journalists/users of Twitter/whistleblowers, etc., who wish to remain anonymous while lawfully exercising their freedom of speech; to unduly record private conversations without consent no matter where they occur; and to track people's movements without their permission or due authorization. The coupling of election votes with personal data, the intentional identification of peaceful protestors, the exposure of the identity of writers/journalists/bloggers/users of Twitter/whistleblowers, etc. against their will, the recording of conversations out in public and the constant tracking of people's movements all risk having a 'chilling effect' respectively on the right to vote, the freedom of assembly, the freedom of speech, freedom of the press, the freedom of movement and thus democracy overall. A threat to privacy, therefore, is also a significant threat to liberty, since privacy and liberty indeed go hand in hand.

Privacy, as Schermer points out, is essentially a negative liberty (2007, p. 121), since it is the *freedom from* undue surveillance, scrutiny and observation, and is often categorized as the 'right to be left alone'. If *knowledge is power*, as Sir Francis Bacon famously first aphorized, then the more knowledge someone knows about another person, the more control he/she can exercise over that person (Schermer, 2007, p. 73). Therefore, since privacy is meant to restrict what an individual or other entity may know or discover about another individual, then privacy can serve as a limit or

---

[22] Available at: http://privacy.org.nz/28th-international-conference-of-data-protection-and-privacy-commissioners

[23] *Ibid*.

[24] Global Privacy Standards for a Global World, The Civil Society Declaration, Madrid, Spain, 3 November 2009, (known as the Madrid Privacy Declaration), available at: http://thepublicvoice.org/madrid-declaration/

constraint on the control governments (or other entities) can exercise over individuals (*Ibid*.). Privacy, on the other hand, is also a positive liberty, since it may endow individuals, for instance, personal autonomy/personal sovereignty, i.e. the *freedom to* take autonomous decisions on their personal/domestic matters (see, e.g., Feldman, 1994).

2.7 THE CONCEPT OF SECURITY

Security is also legally a universal human right.[25] The underlying concept of security is, first and foremost, the protection of persons from injury, harm or termination and, secondly, the protection of objects/property from unlawful/unauthorized damage or destruction. There are various interrelated branches of security and different methods and means of achieving security. In addition to data security,[26] this dissertation predominantly covers public security, aviation security and the security of critical infrastructure (i.e. homeland/national security).

Public security refers to the protection of citizens, which is often a duty of local, regional and national authorities. A variety of threats to public security, for instance, include: murders; armed robberies; kidnappings; deadly virus pandemics; terrorist attacks; and significant natural disasters. Methods and means of helping to maintain public security, for instance, include: the adoption of criminal laws; and the establishment of institutions (e.g. police forces) to enforce the laws and other institutions (e.g. courts) to punish those who violate the law. Other more recent methods and means include the use of technology, such as public surveillance technologies, advanced imaging technologies, forensic technology and ICT infrastructure/applications.

Aviation security refers to the security of airports and aircraft, including the persons onboard, from harm caused by a terrorist attack or hijacking. Aviation security is (primarily) focused on preventing any weapon or explosive device from being brought on board or near an aircraft.[27] Methods and means of achieving aviation security, for instance, include: the screening of passengers and luggage, with the use of technology (metal detectors, X-ray machines, body scanners, etc.) and human resources (i.e. airport security personnel); passenger profiling; and intelligence gathering and analysis.

---

[25] see, e.g., Charter of Fundamental Rights of the European Union (2000), Article 6.

[26] Data security concerns the security of information technology/infrastructures and the information stored thereof.

[27] Though, in the US, for example, aviation security personnel are also heavily focused on preventing any prohibitive item (e.g., lighters, etc.) from being brought on board.

The security of critical infrastructure is an important sub-branch of national security/homeland security. For the most part, the security of critical infrastructure, for instance, includes the protection of nuclear power plants, the electricity transmission/distribution grid, water reservoirs/treatment plants, dams, bridges, airports, seaports, railways, etc. against a terrorist attack or act of sabotage, including from a cyber attack.[28] Methods and means of achieving the security of critical infrastructure, for instance, include: the deployment of police forces, the national/civil guard and other security personnel; the use of physical access control technology; the methods/means used in intelligence gathering and analysis; and cyber security technological measures and procedures.

2.8 PRIVACY, LIBERTY AND SECURITY

The (individual) rights to privacy and personal liberty are not absolute and must be interfered with for the sake of the 'common good' of society (Etzioni, 1999). Security is, indeed, a common or public good, and privacy and liberty, to a certain extent and under certain conditions, have been sacrificed in the name of security. There are certainly plenty of examples where the liberties of individuals have been limited for the sake of security. Law enforcement and national intelligence agencies, for example, have been granted certain authority to collect vast amounts of personal data and infringe upon the right to privacy, in order to prevent a terrorist attack. Online activities/communications are significantly monitored. Global financial transactions are continuously monitored to discover terrorism financing activities. Mobile phones must be capable of being wiretapped by law enforcement agencies and must be capable of revealing the location of where a call is made. At an airport, a patdown or strip search, conducted in accordance with the law and based on the required level of suspicion, is permitted for the purpose of ensuring the security of commercial aviation. And last, but not least, a person's liberty may be taken away, if they have committed a serious crime or significantly interfered with the liberty of another person. As the Constitution Committee of the UK House of Lords sums up, "[n]ational security, public safety, the prevention and detection of crime, and the control of borders are among the most powerful forces behind the use of a wide range of surveillance techniques and the collection and analysis of large quantities of personal data".[29]

---

[28] Cyber security has become absolutely essential for national security and the security of critical infrastructure.

[29] Constitution Committee - Second Report, Surveillance: Citizens and the State (Session 2008-09), para. 45, available at: http://www.parliament.the-stationery-office.com/pa/ld200809/ldselect/ldconst/18/1802.htm

However, given the important merits, as described in section 2.4, privacy is also a common good. Although the right to privacy and other civil liberties are indeed not absolute, and must always be enforced in relation to the common good/general interest of society as a whole, infringements must also be minimized, as far as possible. Moreover, the measures taken to ensure security, which may limit the exercise/enforcement of the right to privacy/data protection, must be both necessary and relative for achieving legitimate objectives (i.e. subject to the principle of proportionality) or needed to protect the freedoms/rights of others, and the limitations must be provided for by law.[30]

Yet, sometimes privacy can potentially conflict with the needs of security and other civil liberties. For example, terrorists could potentially benefit from the vulnerabilities of patdowns, which may result from the legal requirements of bodily privacy and the principle of proportionality. Online anonymity or the incorporation of encryption technologies (a type of Privacy Enhancing Technology) could potentially enhance the ability of terrorists to communicate undetected and to hide behind data protection. Others have similarly pointed out that online copyright infringers, virus disseminators and "cyber-bullies" can hide behind strong data protection rules, which can negatively affect the value of the freedom of expression.[31]

On the other hand, the protection of privacy can also help to ensure security. For instance, the private communications of heads of state, intelligence agents, ambassadors and other government officials are vital for national security, and any breach of this privacy could be detrimental to national or even international security. This was initially a concern, for example, when the mobile phones of the former Prime Minister of Greece, Costas Karamanlis, and several of his cabinet ministers were wiretapped. The secrecy (i.e. privacy) of national intelligence and the concealment of the identity of intelligence agents are also vital for national security. Moreover, the secrecy of the locations, characteristics and vulnerabilities of critical military bases, particularly of

---

30 see, e.g., the Charter of Fundamental Rights of the European Union, Article 52(1).

31 For example, during the post-i2010 Public Hearing on "Priorities for a new strategy for European Information Society" held 23 September 2009 in Brussels, which I attended, a representative from the Creative and Media Business Alliance (CMBA) made the following oral statement: "Some, such as cyber-squatters, spammers, identity thieves, virus disseminators, cyber-bullies and other illegal content providers call for more "data protection" and "safe harbours" on the Internet in the name of freedom of expression and hide behind these but do not respect them themselves". CMBA's full statement is available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/post_i2010/public_hearing/cmba.pdf

Special Forces, and the suppression of the publication of this information are also vital for national security.[32]

Not only is security considered a universal human right in itself, but security is also equally essential for maintaining privacy and other civil liberties/human rights. Without security, there can be no liberty. As Neocleous (2007) and Waldron (2003) both explain, it is not always a matter of balancing security with liberty and it is mistaken to assume that the relation between security and liberty is self-evidently a zero-sum game. In addition, as Neocleous (2007) points out, key classical and contemporary liberal thinkers, including Adam Smith, Thomas Paine and Michel Foucault, equated the liberty of individuals with the security of individuals. Neocleous (2007) also highlights the significance of how Adam Smith (1776) argued "upon impartial administration of justice depends the liberty of every individual, the sense which he has of his own security".[33] Similarly, as Neocleous (2007) additionally highlights, for William Paley (1785), "the loss of security" leads to "the loss of liberty".[34]

Indeed, security and liberty go hand in hand. For instance, public security is crucial for our physical, social and economic well-being and allows for the conditions of prosperity. Data security, which is the protection against unauthorized access to personal data, is absolutely crucial for realizing the right to privacy/data protection. Aviation security both facilitates and enhances the freedom of movement of people, not to mention that it also facilitates international commerce. Public security and the security of critical infrastructure preserve the right to life and the right to lawfully pursue success and happiness.

There is no denying that without security (i.e. aviation security, national/public security, data security, etc.), life, as we know it, at least in the Western world, would essentially not exist. However, privacy can also assist in the maintenance of security, and privacy and other corresponding civil liberties are significant for the pursuit of happiness. Therefore, any legal framework must equally ensure the preservation of privacy and liberty.

---

[32] For example, the recording and recent publication of detailed images of the perimeters of the headquarters of the SAS (British Special Forces) by Google on Street View, including its precise location, has been deemed a serious threat to security by UK military leaders and Members of Parliament. see "Fury as Google puts the SAS's secret base on Street View in 'very serious security breach'" (Daily Mail, 19 March 2010), available at: http://www.dailymail.co.uk/news/article-1259162/Google-Street-View-shows-secret-SAS-base-major-security-breach.html

[33] Smith, Adam. *An Inquiry into the Nature and Causes of the Wealth of Nations* (Methuen & Co., Ltd., 1904, 5th edition, first published 1776), v.1.68.

[34] Paley, William. *The Principles of Moral and Political Philosophy* (R. Faulder, 1785), pp. 444-45.

Particularly, amid the GWOT in a post-9/11 world, the realization of security and the prevention of a terrorist attack merit the sacrifice of privacy and liberty, albeit to a limited degree and under certain controlled circumstances. The key objective then is to identify and implement a balanced and integrated approach for safeguarding privacy, liberty and security in the 21st Century.