ISSN 2029-7564 (online)
SOCIALINĖS TECHNOLOGIJOS
SOCIAL TECHNOLOGIES
2014, 4(2), p. 306–317

PRIVACY IN DIGITAL AGE: DEAD OR ALIVE?! REGARDING THE NEW EU DATA PROTECTION REGULATIONS

Seyed Ebrahim Dorraji
University of Oslo, Norway, s.e.dorraji@student.jus.uio.no

Mantas Barcys
Norwegian Research Center for Computers and Law (NRCCL), Norway,
mantas.barcys@student.jus.uio.no

doi:10.13165/ST-14-4-2-05

Abstract

Purpose *– To review and critically discuss the current state of privacy in the context of constant technological changes and to emphasize the pace of technological advancements and developments reached over the time when the last EU data protection laws came into effect. These facts inevitably affect the perception of privacy and raise the question of whether privacy is dead or takes the last breath in the digital age? This paper is an attempt to address this question.*

Design/Methodology/Approach *– Based on the comparison and systematic analysis of scientific literature, the authors discuss problematic issues related to privacy and data protection in the technology era – where these issues are too complicated to be clearly regulated by laws and rules since "laws move as a function of years and technology moves as a function of months" (Ron Rivest). Therefore, this analytical approach towards the issue may help to facilitate reaching the best-fit decision in this area.*

Findings *– The authors emphasize the change of perception of privacy, which originated and grew on the idea of "an integral part of our humanity", the "heart of our liberty" and "the beginning of all freedoms" (Solove, 2008), leading to the recently raised idea that privacy is severely hanging with threat. The authors are of the opinion that legislation and regulation may be one of the best and effective techniques for protecting*

ISSN 2029-7564 (online)
https://www.mruni.eu/lt/mokslo_darbai/st/apie_leidini/
https://www.mruni.eu/en/mokslo_darbai/st/apie_leidini/index.php

privacy in the twenty-first century, but it is not currently adequate (Wacks, 2012). One of the solutions lies in technology design.

***Research limitations/implications** – The aspects of privacy and data protection in the European Union have been widely discussed recently because of their broad applicability. Therefore, it is hardly possible to review and cover all the important aspects of the issue. This article focuses on the roles of technology and legislation in securing privacy. The authors examine and provide their own views based on the critical analysis of the outstanding scientific material.*

***Practical implications** – The authors highlight the ongoing change of perception of privacy. If regulation is left behind the development of technology, privacy will hardly stay alive. On the other hand, if legislation is applied on an ex-ante basis, technological development will depend on the legislators. The balance of both may be the golden means and it basically depends on the coordinated behavior of all the stakeholders.*

***Value** – The article emphasizes that the rising role of sharp development of technology by itself does not violate privacy. It is the people using this technology and the policies they carry out that create violations (Garfinkel, 2000). In fact, threats, in the first instance, are the consequences of human behavior. In other words, technology can be a significant factor of violating or demolishing privacy, however, it may also be the major method of protecting it. The balance of both may be the key means.*

***Keywords** – data protection, privacy, technology development, consent.*

***Research type** – general review.*

1. Introduction

Privacy and data protection concern everyone and are issues of profound importance around the world. Privacy has been hailed as "an integral part of our humanity", the "heart of our liberty" and "the beginning of all freedoms" (Solove, 2008). This essential component of individual freedom (Blitman, 2012), which allows an individual the opportunity to grow and make mistakes and really develop in a way that he/she cannot do in the absence of it (Sweeney, 2007), faces numerous challenges because of the rapid pace of technological changes. In fact, "Technological advances have allowed personal information to be collected, stored, analyzed, copied and distributed with an ease and level of sophistication that would have been unimaginable when the data protection and privacy acts were passed" (Burrows, 2011).

Nowadays, we are aware that businesses are exploiting personal data for commercial gain by profiling customers in order to improve the marketing of their products and retain their customer base. As Kuneva stated, "Personal information is the new currency of the digital world" (Kuneva, 2009). At the same time, governments are introducing increasingly intrusive electronic surveillance measures to gain information about their own population in the name of public and national security. These factors have convinced some of the scientists that privacy is a dying concept. For instance, Nelson wrote that "Privacy, it seems, is not simply dead. It is dying over and over again". Without a doubt, privacy has been under assault for a decade, from when McNeely famously proclaimed,

"You have zero privacy anyway. Get over it" (McNealy, 1999), to when Facebook's founder Mark Zuckerberg stated that no expectation of privacy is part of "current social norms".

All this inevitably raises the question of whether privacy is dead or is taking its last breath in the world. To address this question, first of all, the authors of the paper evaluate the situation of privacy in the digital age by examining emerging new technologies and their effects. Secondly, the authors take a look at the current EU Data Protection Directive 95/46/EC and its new framework which has been updated to reflect technological and market developments and could make an important contribution to global harmonization efforts, and could also lead global privacy regulations in the 21st century. Finally, the authors present some new ideas for strengthening privacy in the technology age and also analyze whether a comprehensive privacy statute is adequate for dealing with new developments, or whether some other solutions and measures to protect our privacy in this new era are needed.

2. Definition of Privacy

Privacy, as a fundamental human right, has been protected under multinational privacy guidelines, directives and frameworks in different countries or conventions at international level, such as the United Nations Universal Declaration of Human Rights of 1948 (Article 12), International Covenant on the Civil and Political Rights (Article 17) and The European Convention of Human Rights of 1950 (Article 8) since 1950s.

However, beyond this worldwide consensus about the importance of privacy and data protection, there is no universal definition of it (Kasneci, 2008). The common law concept of privacy is often traced back to American scholars Warren and Brandeis' famous essay of 1890, in which they described privacy as "the right to be let alone" (Warren and Brandeis, 1890). Nevertheless, every scholar looks at privacy from its specific perspective. For instance, Boyd said that "Fundamentally, privacy is about having control over how information flows" (Boyd, 2010). One of the most popular definitions of privacy was written by Westin. He stated that "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1970). According to Solove, "Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations […]" (Solove, 2008).

3. Privacy and Technology Developments

3.1. Technological Challenges Posed to Privacy

Froomkin stated that "The rapid deployment of privacy-destroying technologies by governments and businesses threatens to make informational privacy obsolete"

(Froomkin, 2000). Satellites monitoring, growing automated surveillance and personal smart phones may track every movement of the individual. Radio Frequency Identification (RFID) systems and online purchases are revolutionizing personal information usage and have consequently started to re-shape our understandings of privacy and our requirements of privacy laws (Burdon, 2012).

These emerging technologies have forced us to ask a very important question: Is technology destroying our precious privacy? Blaming technology for the death of privacy is not new. In 1890, Warren and Brandeis argued that privacy was under attack by "recent inventions and business methods". They contended that the pressures of modern society required the creation of a "right of privacy", which would help protect what they called "the right to be let alone" (Garfinkel, 2000).

Technology is involved in various privacy problems, as it facilitates the gathering and processing of information. When individuals browse the web, use their smartphones and make online transactions, they leave data crumbs everywhere. Technology, nevertheless, by itself does not violate our privacy. It is the activities of people using this technology and the policies they carry out that create violations (Garfinkel, 2000). Normally, individuals consistently share personal information about themselves and post pictures and videos online. With smart phones becoming commonplace, people can be easily tracked because they are willingly giving up their location information. Besides, we associate with 'friends' who do not take our privacy seriously and, as Syrus said, "shout our private matters from the rooftops". This is an excellent message in this era of social media. We tend to blame technology for our loss of privacy, but why do that if we refuse to take our own privacy seriously? (Bloem, Duivestein, Manen, Doorn and Ommeren, 2012)

The merits or defects of particular technologies are not inherent in the technologies themselves, but rather, depend on how they are used and, above all, on how closely their use is monitored and accounted for by the parties involved (Etzioni, 2007). Therefore, it should be noted that the burden is also on us to protect our privacy by keeping our location private, avoiding certain habits, such as sharing personal information on social networking sites, and seeking out encryption programs to protect our data. To sum up, we are eager to allow the social and economic potential of technology to flourish as an everyday part of our lives. But the fear of privacy loss, uncertainty and doubt as consequences of the large-scale application of technology carry a huge inherent risk. All stakeholders involved must accept responsibility here (Bloem, Duivestein, Manen, Doorn and Ommeren, 2012).

3.2. Does Technology Protect Privacy?

It is true that technology is advancing to track our every move, often without our knowledge. But the technology is also advancing to protect privacy in ways that were not available before (Rounds, 2011). For instance, encryption technologies can protect data from unauthorized access (Whitten and Tygar, 1999). Moreover, Digital Rights Management (DRM) technologies can allow conditional access to encrypted information, tracking and allowing usage on a per-user and per-device basis (Traw, 2003).

Some scholars, such as Garfinkel, believe that although it is possible to use technology to protect or enhance privacy, the tendency of technological advances is to do the reverse.

He said that "By its very nature, technology is intrusive". Unfortunately, as Assange alluded, "much of the technological effort is aimed at invading privacy". While attention is often focused on the privacy challenges of the digital environment, technology also brings new opportunities to offer individuals practical options to participate in the protection of their privacy. The balance between Privacy-Invasive Technologies (pits) on the one hand and Privacy-Enhancing Technologies (pets) on the other is changing continuously (Etzioni, 2007). This fundamental and integral approach is known as "Privacy by Design". This concept will be explored in section 6 of this paper.

4. European Data Protection Law

4.1. Data Protection Directive versus New Society

The current EU Data Protection Directive 95/46/EC was passed in 1995, establishing one of the most rigorous and extensive data protection regimes in the world and setting out some strong basic principles with the aim of protecting the fundamental rights and freedoms of individuals, including their privacy and personal data.

The context in which the data protection directive was created has been changed fundamentally.

The directive was showing its age since it did not consider important aspects, such as globalization (cross-jurisdiction data protection), technological developments, such as technology convergence, social networks, and cloud computing sufficiently. So, new guidelines and amendments for data protection and privacy were required. Therefore, a proposal for the regulation was released on 25 January 2012. The proposal encompasses two main elements: a draft regulation, dealing generally with data protection (the General Data Protection Regulation), and a draft directive relating to the processing of personal data within the criminal justice system.

4.2. Analyzing the New EU Data Protection Framework

Modernizing the EU legal system for the protection of personal data in all areas of the Union's activities to meet the challenges resulting from globalization, the use of new technologies, and the needs of public authorities, in order to improve current data protection legislation as well as the effective application of data protection principles, is a concrete step to reinforcing privacy in a new age: the so-called "digital age" (Craig and Ludloff, 2011). According to Reding, "The framework, which applies to all 27 European member states, is a critical piece of legislation for growth and strength that is fit for the digital age and will encourage the development of new services" (Reding, 2012).

There are numerous key changes in the reform which strengthens the privacy and the rights of individuals. For instance, the new framework is aimed at ending the increasing number of data breach scandals by requiring organizations to notify the national data protection authority and all individuals affected by a data breach within 24 hours. Also, individuals would have the right to require that organizations delete their data under certain circumstances, "without delay", where there is no legitimate interest in retaining

it. Significant penalties may apply if the data controller fails to act promptly. This is commonly referred to as the "right to be forgotten". Moreover, there are many other positive reforms, such as data processors' obligations; however, reviewing all of them is beyond the scope of this article. Ultimately, it is worth highlighting that the new EU Data Protection Framework which strengthens individual rights and tackles the challenges of globalization and new technologies will enable us to protect our privacy more effectively. It has a pivotal role since "Without an innovative renewal of data protection law freedom will diminish in such an unnoticed way as clean water and air" (Sólyom, 1988).

5. Consent as a Part of the Privacy Policy

On the face of it, there is currently a great in-depth debate of the rules by legislators, legal academics and practitioners on the European Union's move to harmonize data protection regulation across the EU. To look deeper into the proposal, it becomes clear that the EU wants more than just a reduction of bureaucracy – it is trying to force a change in the mindset of organizations regarding how to manage our personal data (Glick, 2012).

The European Commission has proposed and the European Parliament has approved a comprehensive reform of the EU Data Protection Directive 95/46/EC (hereinafter – Directive) to strengthen online privacy rights and boost Europe's digital economy. The proposal – which is going to be adopted in 2014 (with a two year transitional period before it comes into force) – introduced a single set of rules giving individuals more control over how to use and manage their personal data. One of the fundamental principles reflecting the efforts to enhance privacy in the EU is consent. The in-depth analysis of consent requirement has been chosen due to its impact on derivative right arising in the proposed legislation (e.g., a right to be forgotten, a right to easier access to own data, etc.). Although the EU approach emphasizes the requirement to provide consumers with enough information to enable the consumer to provide his consent, there is no comprehensible threshold to determine the point at which the consent becomes valid. However, the consent framework is going to be significantly modified by the proposed regulation, which gives broader definitions and conditions of consent compared to the Directive.

However, any structure of consent must recognize that it is not easy to develop a uniform approach that works in all circumstances or contexts. At the same time, consent inevitably has to be somewhat flexible in practice with a broader definition and clear conditions of consent, making the elements that constitute valid consent clearer and easily applicable.

5.1 Change of the Consent Requirement

Following the current EU legislation, consent constitutes the general rule although data may be processed without it if necessary (Directive, Art. 7). Current legislation requires that a person's consent for processing the individual's personal data should be a

freely given specific and informed indication of his wishes by which the individual signifies his agreement to this data processing. However, there is no clear and unambiguous clarification of such a term and Member States interpret it differently. Unfortunately, in some cases current regulations do not provide clearly what would constitute freely given, specific and informed consent to further data processing. Clarification related to the conditions for the data subject's consent have to be provided, in order to guarantee informed consent and to ensure that the individual is fully aware that he or she is consenting, and exactly to what data processing he or she is consenting. Clarity on key concepts can also favor the development of self-regulatory initiatives to develop practical solutions consistent with EU law (Communication from the Commission, COM (2010)). Apparently, the consent framework is going to be significantly modified by the regulation, which gives broader definition and conditions of consent compared to the Directive.

The Commission's proposed regulation continues to recognize consent as a legitimate basis for both processing personal data as well as transferring it outside the EU. Conversely, it also provides more narrow means of obtaining a valid consent, as well as imposing additional conditions on their use. According to the regulation, consent is any "freely given specific, informed and explicit indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed" (Art. 4(8)). The reference to '*freely given, informed and explicit*' attributes is clearer than the precedent '*unambiguously*' consent. However, the concept of the regulation creates an odd reference to the 'wishes' through which the data subject confirms the agreement to data processing. A wish is a desire and it is clear that people wish, desire to access new services, to amplify their experience with new technologies and applications, etc. Nevertheless, a wish is not synonym of will, which is a deliberate choice that produces legal consequences. Will, rather than wishes, is at the heart of a data protection regime (Costa, 2012).

Moreover, Article 7(4) of the Regulation establishes welcome procedural and substantive conditions, embracing the proportionality principle approach. Consent should never provide a legal basis where there is a '*significant imbalance*' between the parties. It is questionable what a "significant imbalance" is and whether the concept should be imported into data protection law. It seems to be rare that individuals enjoy an equal bargaining position with the various, typically corporate, entities that solicit their consent. Injecting the notion of 'significant imbalance' into the law is, therefore, potentially dangerous and could threaten the utility of consent (Cooper, 2011). Current legislation does not directly regulate revoking of the consent, but it arises from the broad interpretation of legal norms and case law practices. However, the method of obtaining and revoking consent is explicit and appropriate to the particular circumstances in the proposed regulation.

In turn, relying on the so-called legitimate interests ground to process personal data has become much more difficult, as controllers must then inform individuals about such specific processing and the reasons why those legitimate interests override the interests or fundamental rights and freedoms of the individual. Another interesting point is that explicit consent must be obtained from data subjects. It will not be acceptable to

assume consent from a data subject's silence or inactivity or through generic terms and conditions (Recital 25 in proposed Data Protection Regulation).

5.2. Pros and Cons of the Changes

The legal approach, which consists of an '*opt-in*' idea, usually requires the person's consent before personal information is processed. It follows immediately from both the proposed and current legal text that the information should be given before the user's consent (European Data Protection Supervisor, 2011). In this way, current EU legislative approach, in the line with the proposed one, provides individuals with broad protections that emphasize the opt-in, as opposed to the opt-out, model.

As a result, the *opt-in* approach effectively prevents firms from disseminating information about its customers and consequently blocks data sharing. On the other hand, placing restrictions on, for example, personalized advertising will be beneficial to the consumer if it limits price discrimination. As companies possess more information, they have a greater ability to price discriminate (e.g., offer personalized prices based on their information about the consumer's budget and spending habits). Therefore, placing restrictions on behavioral advertising limits the ability of businesses to charge higher prices by targeting those customers with a higher marginal willingness to pay. The restrictions that the proposed EU legislation places on personalized advertising should lead to a culture where direct marketing is focused on those who have requested it, preventing consumers being presented with marketing which they do not want (UK Ministry of Justice, 2012).

To sum it up, it is obvious that technological developments also require a careful consideration of consent. Giving the data subjects a stronger voice '*ex ante*', prior to the processing of their personal data by others, however, requires explicit consent (and therefore an opt-in) for all processing that is based on consent (contrary to law U.S. approach). On the other hand, red tape will be cut by imposing new legislation, thus saving businesses an estimated € 2.3 billion a year, and companies will only have to deal with a single national data protection authority in the EU country where they have their main operations (European Commission Website, 2012).

6. Ideas for Strengthening Privacy in Digital Age

Legislation and regulation may be one of the best and effective techniques for protecting privacy in the twenty-first century, but is it adequate? (Wacks, 2012) Do we need some other solutions and measures to protect our privacy in the digital age? The law is a crucial instrument in the protection of privacy (and it is locked in a struggle to keep pace with the relentless advances in technology), but that is not sufficient. As Rivest said, "You know, the problem with trying to solve these problems with laws is that laws move as a function of years and technology moves as a function of months."

So, what is the solution? One of the solutions lies in the technology design or in a broader concept 'Privacy by Design'. Privacy by Design is "the use of technical and

organizational measures in information systems to avoid invasions of people's personal privacy. If information systems are inherently privacy-friendly, this considerably adds to a sustainable information society" (Bloem, Duivestein, Manen, Doorn and Ommeren, 2012). For instance, one of the first things that should be done is to train the engineers and computer scientists who are involved in the building and development of technology, to create technology with a specific and strong privacy panel because it is so much affordable and easier for society if the new technology rolls out with privacy controls in them (Sweeney, 2007)

6.1. Privacy by Design

Privacy by design is a nebulous concept. It advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks (Cavoukian, 2009). The concept of Privacy by Design is explicitly based on Privacy-Enhancing Technologies (pets). The British Information Commissioner's Office describes pet as "any technologies that protect or enhance an individual's privacy, including facilitating access to their rights under the Data Protection Act." Therefore, the use of pets can help "design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules making breaches more difficult and/or helping to detect them." For instance, Microsoft has now operationalized a technological Privacy by Design solution that guarantees the quality of digital data for targeting by organizations, while making individual people untraceable with absolute certainty. In Big Data circles, the method is known as Differential Privacy (Bloem, Duivestein, Manen, Doorn and Ommeren, 2012).

To conclude, it is worth mentioning that to protect our privacy in the digital age, seven basic principles around the core of each technology, design and infrastructure, and the operation itself have been proposed by Ann Cavoukian, 'mother' of Privacy by Design.

"1. Privacy by Design means that you take proactive and preventive action: not re-active.
2. Privacy guarantee needs to be the default setting.
3. Privacy needs to be embedded in the design.
4. Go for full functionality: not a poor trade-off but a clearly positive balance.
5. Solutions need to be totally conclusive and unequivocal: end-to-end security at all times.
6. Ensure full visibility and transparency: openness is your leitmotiv.
7. Deal with privacy respectfully: particularly by focusing attention on the individual" (Cavoukian, 2009).

7. Conclusion

Undoubtedly, advances in civilization and in technology have profoundly changed the world around us, brought new challenges for the protection of personal data and

"cultivate new sensibilities and vulnerabilities toward invasions of privacy" (Bakke, 2006). The risks of this type of technology need to be understood so that we can fully gain its benefits. As O'Harrow has written, "More than ever before, the details about our lives are no longer our own, they belong to the companies that collect them and the government agencies that buy or demand them in the name of keeping us safe." Does that mean the anonymity and privacy that we take for granted have disappeared? Or, as Rambam argued, that privacy is dead and should we get over it?

The death of privacy has been predicted forever. More and more people are saying that we should just forget all about our privacy; after all, "something like privacy simply no longer exists in this age of technology, where everyone is open to surveillance at all times; where there are no secrets from government" (Bloem, Duivestein, Manen, Doorn and Ommeren, 2012). We have been saying this for generations, but it turns out it is not necessarily true. Definitely, we need both technical and legal protections appropriate to the circumstances of time. Otherwise, as O'Harrow declared, rather than having "nothing to hide", we will have "no Place to hide" (O'Harrow, 2006). Cultivating one's awareness and individual responsibility is also a matter of importance.

Ultimately, it is needless to point out that privacy is not dying. Without a doubt, it is hanging by a thread. We believe that Privacy by Design, Privacy-Enhancing Technologies and standardized legislation, such as the new EU Data Protection Framework, in addition to corresponding responsible behavior, all constitute the integral approach that should enable us to protect our privacy in the technology era (Bloem, Duivestein, Manen, Doorn and Ommeren, 2012).

Reference

Bakke, S. *Privacy, Control, and the Use of Information Technology: The Development, Validation, and Testing of the Privacy-Invasive Perceptions Scale*. Kent State University, 2006 [interactive]. [accessed on 12-02-2014]. <https://etd.ohiolink.edu/ap/10?0::NO:10:P10_ACCESSION_NUM:kent1145192698>.

Bloem, J.; Doorn, M.; Duivestein, S.; Manen, T.; Ommeren, E. *Privacy, Technology and the Law: Big Data for Everyone through Good Design*. VINT research report 3. The Sogeti Trend Lab VINT, 2013 [interactive]. [accessed on 15-02-2014]. <http://blog.vint.sogeti.com/wp-content/uploads/2013/04/VINT-Big-Data-Research-Privacy-Technology-and-the-Law.pdf>.

Burdon, M. *Securing Your Privacy Online*. 2012 [interactive]. [accessed on 07-02-2014]. <http://www.uq.edu.au/graduatecontact/2012/general/securing-your-privacy-online/>.

Blitman, A. *Why Privacy Is Dead*. 2012 [interactive]. [accessed on 07-02-2014]. <http://thewrittenblit.com/2012/08/02/why-privacy-is-dead/>.

Cavoukian, A. *Privacy by Design*. 2009 [interactive]. [accessed on 12-02-2014]. <http://www.ipc.on.ca/images/Resources/privacybydesign.pdf>.

Craig, T., and Ludloff, M. *Privacy and Big Data*. 2011.

Cooper, D. *Consent in EU Data Protection Law*. 2011 [interactive]. [accessed on 12-02-2014]. <http://www.europeanprivacyassociation.eu/public/download/EPA%20Editorial_%20Consent%20in%20EU%20Data%20Protection%20Law.pdf>.

Costa, L., and Poullet, Y. Privacy and the Regulation of 2012. *Computer Law & Security Review*. 2012, 28(3) [interactive]. [accessed on 08-02-2014]. <http://www.sciencedirect.com/science/article/pii/S0267364912000672>.

Curren, L., and Kaye, J. Revoking Consent: A 'Blind Spot' in Data Protection Law? *Computer Law & Security Review*. 2010, 26(3) [interactive]. [accessed on 15-12-2014]. <http://www.sciencedirect.com/science/article/pii/S0267364910000488>.

Data Protection Working Party, Opinion 15/2011 on the Definition of Consent. 2011 [interactive]. [accessed on 19-02-2014]. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>.

European Data Protection Supervisor. *Social Networks and Data Subject Consent*. 2011 [interactive]. [accessed on 10-02-2014]. <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2011/11-07-05_Consent%20in%20Goettingen_EN.pdf>.

European Commission. *Stakeholders' Consultations "Future of Data Protection"*. Backgroud Paper. <http://ec.europa.eu/justice/news/events/data_protection_regulatory_framework/ background_paper_en.pdf>.

European Commission. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union*. Brussels, 4.11.2010 COM (2010) 609 final [interactive]. [accessed on 15-02-2014]. <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>.

European Commission. *Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data* [interactive]. [accessed on 15-02-2014].

European Commission Website. More Safeguards for Online Privacy Rights – 25/01/2012 [interactive]. [accessed on 19-02-2014]. <http://ec.europa.eu/news/business/120125_en.htm>.

Etzioni, A. *Are New Technologies the Enemy of Privacy*. 2007.

Finney, G. *Privacy Is Dead. Now Where Is My Inheritance?* 2013 [interactive]. [accessed on 12-02-2014]. <https://www.secureworldexpo.com/blog/privacy-is-dead-now-where-is-my-inheritance>.

Froomkin, A. M. The Death of the Privacy? *52 Stanford Law Review*. 2000.

Garfinkel, S. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly & Associates, Inc., 2000.

Glick, B. *Compliance and Risk. IT in Europe*. Volume 4. 2012 [interactive]. [accessed on 19-02-2014]. <http://docs.media.bitpipe.com/io_10x/io_106016/item_566346/IT%20in%20Europe_final.pdf>.

Gourlay, D., and Gallagher, D. *Proposed Changes to the EU Data Protection Regime: What You Need to Know*. 2011 [interactive]. [accessed on 07-02-2014]. <http://www.mcclurenaismith.com/assets/publications/ebulletins/DP%20Regulation%20Article%20template.pdf>.

Hultsch, C. Basic Principles of European Union Consent and Data Protection. *Technology Law Source*. 2011 [interactive]. [accessed on 12-02-2014]. <http://www.technologylawsource.com/2011/07/articles/privacy-1/basic-principles-of-european-union-consent-and-data-protection/print.html>.

Kang, C. *Is Internet Privacy Dead? No, Just More Complicated*. 2010 [interactive]. [accessed on 09-02-2014]. <http://voices.washingtonpost.com/posttech/2010/03/is_internet_privacy_dead_no_ju.html>.

Kasneci, D. *Data Protection Law: Recent Development*. PhD Thesis. 2008.

Lipschultz, J.H. *Privacy Is Dead – Really?* [interactive]. [accessed on 10-02-2014]. <http://www.huffingtonpost.com/jeremy-harris-lipschultz/online-privacy_b_1831956.html>.

O'Harrow, R. *No Place to Hide*. Free Press, 2006.

Rauhofer, J. Privacy Is Dead, Get over It! Information Privacy and the Dream of a Risk-free Society. *Information & Communications Technology Law*. 2008, 3(17).

Rounds, B. *Is Privacy Dead?* 2011 [interactive]. [accessed on 09-02-2014]. <http://www.howtovanish.com/2011/12/is-privacy-dead/>.

Rosen, D. *Is Privacy Dead? 4 Government and Private Entities Conspiring to Track Everything You Do Online and off*. 2012 [interactive]. [accessed on 10-02-2014]. <http://www.

alternet.org/civil-liberties/privacy-dead-4-government-and-private-entities-conspiring-track-everything-you-do>.

Solove, D.J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

Traw, C.B.S. *Technical Challenges of Protecting Digital Entertainment Content*. 2003.

UK Ministry of Justice. *Impact Assessment on Proposal for an EU Data Protection Regulation*. 22.11.2012 [interactive]. [accessed on 19-02-2014]. <http://www.huntonprivacyblog.com/wp-content/uploads/2012/11/UK-Govt-Impact-Assessment.pdf>.

Wacks, R. *Privacy: A Very Short Introduction.* 2012 [interactive]. [accessed on 12-02-2014]. <http://blog.oup.com/2012/06/is-privacy-dead-vsi/>.

Warren, S.D., and Brandies, L.D. The Right to Privacy. *Harvard Law Review*. 1890, 5(6).

Warwick, A. *EC Publishes Proposed Data Protection Reforms.* 2012 [interactive]. [accessed on 12-02-2014]. <http://www.computerweekly.com/news/2240114326/EC-proposes-a-comprehensive-reform-of-data-protection-rules>.

Westin, A.F. *Privacy and Freedom*. 1970.

Whitten, A., and Tygar, D. *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. In Proceedings of the 8th USENIX Security Symposium, Washington, DC, 1999 [interactive]. [accessed on 10-02-2014]. <http://ec.europa.eu/justice/news/events/data_protection_regulatory_framework/background_paper_en.pdf>.

Wright, J., and Chatfield, T. *As Google Acts, the Question Is: Have We Lost Our Privacy to the Internet?* 2012 [interactive]. [accessed on 10-02-2014]. <http://www.guardian.co.uk/technology/2012/mar/03/internet-privacy>.

Walter, Ch. *Privacy Isn't Dead, or At Least It Shouldn't Be: A Q&A with Latanya Sweeney*. 2007 [interactive]. [accessed on 10-02-2014]. <http://www.scientificamerican.com/article.cfm?id=privacy-isnt-dead>.