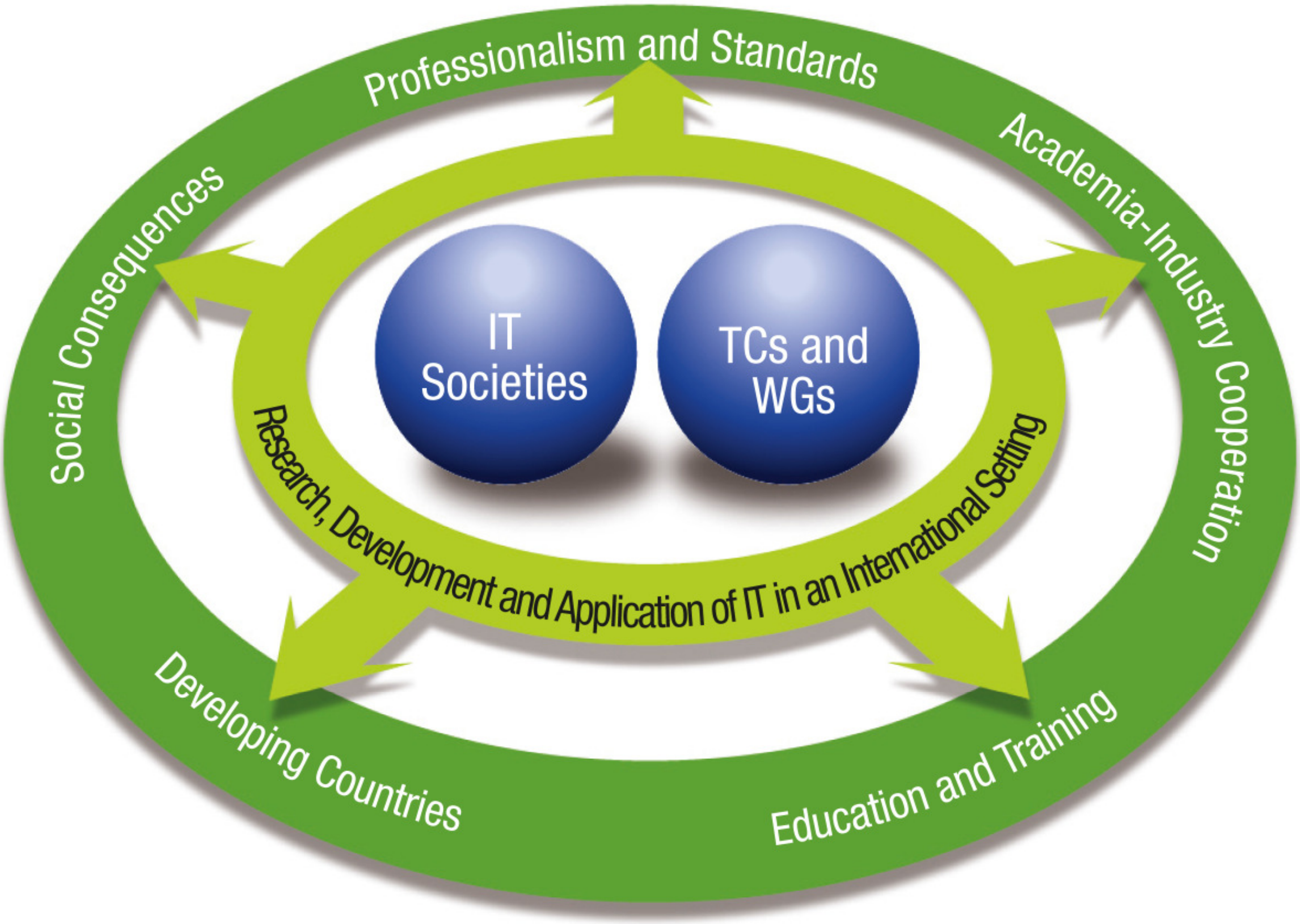
novática
Revista de la Asociación de Técnicos de Informática
SPECIAL ISSUE 2012-2013 Annual Selection of Articles

Privacy and New Technologies

International Federation for Information Processing

Hofstrasse 3, A-2361 Laxenburg, Austria
Phone: +43 2236 73616 Fax: +43 2236 736169
E-mail: ifip@ifip.org   http://www.ifip.org


Professionalism and Standards
Academia-Industry Cooperation
Education and Training
Developing Countries
Social Consequences
Research, Development and Application of IT in an International Setting
IT Societies
TCs and WGs

IFIP is the global forum of ICT experts that plays an active role in developing and offering expertise to all stakeholders of the information and knowledge society

novática
Revista de la Asociación de Técnicos de Informática

Novática, founded in 1975, is the oldest periodical publication amongst those specialized in Information and Communications Technology (ICT) existing today in Spain. It is published by **ATI** (*Asociación de Técnicos de Informática*) which also publishes **REICIS** (*Revista Española de Innovación, Calidad e Ingeniería del Software*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI is a founding member of **CEPIS** (Council of European Professional Informatics Socities), an organization with a global membership of above 200,000 European informatics professionals, and the Spain's representative in **IFIP** (International Federation for Information Processing), a worldwide umbrella organization for national societies working in the field of information processing. It has a collaboration agreement with **ACM** (Association for Computing Machinery) as well as with **AdaSpain**, **AI2**, **ASTIC**, **RITSI** and **Hispalux** among other organisations in the ICT field.

Editorial Office, Advertising and Madrid Office
Plaza de España 6, 2ª planta, 28008 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Layout and Comunidad Valenciana Office
Av. del Reino de Valencia 23, 46005 Valencia; Tlfn. 963740173 <novatica_prod@ati.es>
Accounting, Subscriptions and Catalonia Office
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>; <novatica.subscripciones@atinet.es>
Aragón Office
Lagasca 9, 3-B, 50006 Zaragoza Tlfn./fax 976235181 <secreara@ati.es>
Andalucía Office <secreand@ati.es>
Galicia Office<secregal@ati.es>
Advertising Plaza de España 6, 2ª planta, 28008 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Legal deposit: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Cover Page: Dancing House - Concha Arias Pérez / © ATI
Layout Design: Fernando Agresta / © ATI 2003

Special English Edition
2012/2013 Annual Selection of Articles

summary

editorial

From the Chief Editor´s Pen

monograph

Privacy and New Technologies

Guest Editors: Gemma Galdon Clavell and Gus Hosein

editorial

Novática: Reaching beyond International Borders

Since the first appearance of ***Novática*** in 1975 its publisher (ATI - *Asociación de Técnicos de Informática*) made the decision of keeping the contents of this journal evolving permanently at the pace of the times.

Thus, if you look at the issues published in the initial years[1], you could observe a special emphasis on the dissemination of the knowledge about the then young information technologies, as well as the training of new professionals and the creation of a community of IT professionals in Spain. This is in contrast with later and current issues, whose main aim is the dissemination of scientific and technical advances in the IT field as well as the analysis of high-level contemporary social and business debates related to Information Technologies.

The same happens in relation with the scope of our journal. In its infancy, Novática, which is published in Spanish, was essentially local and now it is essentially global speaking in terms of authors, subjects and even readership. The main proof of that is our successful partnership with CEPIS, the Council of European Professional Informatics Societies, to create and edit its journal UPGRADE, published in English, which lasted from 2000 to 2011.

For that reason, ATI has decided to publish an English edition of ***Novática***, at least on a yearly basis. These editions will include a selection of articles published in Spanish in the last months. I would like to point out that this is the reaffirmation of our international vocation which we intend to reinforce in the near future.

It is my pleasure to announce to you that for this 2012-2013 Selection of Articles we have made the choice of publishing an, in our opinion, highly interesting monograph on "Privacy and New Technologies" whose articles have been published in Spanish during 2012 and 2013.

As our Chief Editor's article states, this monograph deals with a very important subject which gives rise to a widespread social, legal and even philosophical debate in which Information Technologies and their evolution play an essential role.

On behalf of ATI and its thousands of members thank you very much to everybody who has contributed to make it possible.

Dídac López Viñas,
President of ATI

[1] See <http://www,.ati.es/novatica/indice.html>.

From the Chief Editor´s Pen

Privacy: Our Contribution to a High-Level Debate in the Digital Age

If someone asked about a paradigmatic concept to illustrate how IT contribute to social changes a very likely answer would be "privacy".

Indeed, I would say that this is a social concept that remained relatively static for ages, even in the first stages of the new digital era.

It has been since the Internet boom that the old ideas, habits, laws and regulations have been shaken up and somehow forced to evolve. As a consequence new models of privacy can be considered as a 21st century issue which is giving rise to a dynamic, vigorous and exciting debate. With special mention to the dynamism of this process as the power of new technologies is continuously growing and technology within reach of people is spreading in a seemingly unstoppable way.

Two of the most influential factors in this pervasive environment are communication technologies and surveillance technologies. Nowadays as almost everybody in the developed world can spend all his/her time connected both at work and at home, governments and regulators feel the need to control those processes to prevent potential dangers.

In the meanwhile offenders and privacy abusers both private and public (let's remind the recent "Snowden case") have taken advantage of the increasing sophistication of the aforementioned technologies and the lack of technical knowledge of the average citizen for perpetrating their misdeeds.

As a consequence, the dichotomy between privacy and safety is setting up one of the most exciting, thrilling and widespread debates in the digital age whose participants range from governments, regulators and judges to businesses, individuals and ad-hoc associations.

In this context, we consider fully justified our choice of the "Privacy and New Technologies" monograph for the "2012-2013 Selection of Articles", a special edition of ***Novática*** in English which is based mainly on the monograph on the same subject published in Spanish by our journal in 2012.

The work accomplished by the guest editors of the monograph, ***Gemma Galdon Clavell*** and ***Gus Hossein***, prestigious scholars and active privacy avdocates has been outstanding, as well as the articles written by authors with very high expertise on the subject matter. Many sincere thanks to all of them.

We also kindly thank our English Editors (***Arthur Cook***, ***David Cash***, ***Roger Shlomo-Harris*** and ***William Centrella***) for their contribution to this issue as well as the other English Editors who have been regularly assisting us with our publications in English.

We expect that our readers will find the articles interesting and hope thus to make our contribution to this exciting debate.

Llorenç Pagés Casas,
Chief Editor of Novática

CEPIS
Council of European Professional
Informatics Societies

The **European Network** for **Informatics Professionals**

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among informatics professionals in recognition of the impact that Informatics has on employment, business and society.

CEPIS represents over 350,000 ICT and informatics professionals through the national computer societies that are its members in 32 countries in Europe and beyond.

Ensuring the development and maturation of ICT professionalism in Europe is key concern of CEPIS. In addition, CEPIS engages in a number of activities linked to its mission including e-skills and digital literacy, education, women in ICT, green ICT, and research, development and innovation.

www.cepis.org

Connect with CEPIS on social media

twitter.com/cepis_europe

linkedin.com/company/cepis

Gemma Galdon Clavell[1], Gus Hosein[2]

[1]Sociology Department, University of Barcelona; Member of the Advisory Board of Privacy International; [2]Executive Director at Privacy International

<gemma.galdon@gmail.com>, <gus@privacy.org>

Presentation
Privacy, Technology and Policy: Social Networks, Data Mining and Surveillance

Guest Editors

Gemma Galdon Clavell is a policy analyist working on surveillance, the social, legal and ethical impact of technology, smart cities, privacy, security policy, resilience and policing. She is currently working as a researcher at the Sociology Department at the Universitat de Barcelona (UB), where she is a leading partner and member of several research projects, such as Increasing Resilience in Surveillance Societies (IRISS -FP7), Living in Surveillance Societies (LiSS -COST) and the Virtual centre of excellence for research support and coordination on societal security (SOURCE -FP7). She completed her PhD on surveillance, security and urban policy in early 2012 at the Universitat Autònoma de Barcelona (UAB), where she also got an MSc on Policy Management, and was later appointed Director of the Security Policy Programme at the Universitat Oberta de Catalunya (UOC). Previously, she worked at the Transnational Institute (TNI), the United Nations' Institute for Training and Research (UNITAR) and the Catalan Institute for Public Security (ISPC). She teaches at several foreign universities, mainly Latin-American, and is a member of the IDRC-funded Latin-American Surveillance Studies Network (LASSN). Additionally, she is a member of the international advisory board of Privacy International and a regular analyst on TV, radio and print media. Her recent academic publications tackle issues related to the proliferation of surveillance in urban settings, urban security policy and community safety, security and mega-events and the relationship between privacy and technology.

Gus Hosein is the Executive Director at Privacy International. For over fifteen years he has worked on the intersections of technology and human rights. He has acted as an external evaluator for UNHCR, advised the UN Special Rapporteur on Terrorism and Human Rights, and has advised a number of other international organisations. He has held visiting fellowships at Columbia University and the London School of Economics and Political Science. He has a B.Math from the University of Waterloo and a PhD from the University of London. He is a Fellow of the Royal Society for the encouragement of Arts, Manufactures and Commerce (FRSA).

Our modern popular conceptualization of technology is that it is transformative. Smart devices transform the way we live our lives. Social networking transforms the way we communicate. Search engines transform the way we seek out information. Interactive news services transform the way we consume information [1][2]. In turn, so the argument goes, our lives transform. Our markets, our caretakers, and our governments are all different now because of technology. As a result, according to this conceptualization, our expectations and demands are changed, perhaps radically. But if our expectations change, do our rights also change? Is our right to own the data we produce and our own image also altered by technological developments?

This dynamic relationship between technology and its impact on our societies finds an exciting arena in the debates around our right to our personal data and our privacy. Even though some have rushed to conclude that 'privacy is dead' or is no longer a social norm[1] , the amount of discussions, forums and policy papers being generated around the need to conceptualize and regulate privacy is just fascinating. Contrary to what some like to assert, therefore, privacy is emerging as one of the key themes of the 21st Century, and the ramifications of the discussion reach areas as diverse as the law, politics and policy, technology and society [3][4][5].

In one of the most well-known and accepted definitions, privacy is explained as the right or capacity to protect our private life from outside interference. However, while only a few decades ago the body, the physical person and personal identity were all in one, today the proliferation of all kinds of technological artifacts and of data exchange at all levels has multiplied the amount of dimensions we need to take into account when attempting to define what are the limits of our 'private space'. This constitutes an important conceptual change, and it has implications that run wide and deep in a myriad of disciplines and practices, from law to public policy, including technological development, design and the limits of the public and private spheres.

However, this is not a new debate. In the 1990s, some argued that privacy was a selfish right that needed to be reconsidered in a modern world, as modern technologies perhaps allowed too much privacy [6]. In the early 2000s the debates around the world were about how privacy is a far secondary issue to the greater needs of national security [7][8]. In the past few years, the narrative has been that privacy is an inhibitor to trade in the form of advertising in exchange for free services, or an old social value, unfit for a world where we all embrace social networking and the routine, voluntary exposure of our personal data. The use and abuse of the term, thus, has not translated into a better understanding, conceptualization and adaptation of the term to the new realities. This is one of the issues we want to tackle with this special edition of ***Novática***.

Our goal, however, is not to praise privacy - nor are we here to bury it. Rather, the study of privacy may provide us with richer conceptualisations of modern technology and modern society, at least richer than the pervasive 'transformative' discourse we have seen to date. Like all domains involving humans and objects, privacy debates and discourses are full of incoherence and inconsistencies that beautifully limit our abilities to draw simple narratives. Perhaps our goal should be to prevent simple narratives. In order to move away from these simple narratives, in this opening piece we hope to identify some of the limitations that emerge from more detailed readings of privacy challenges in the face of technology developments.

That is not to say that we do not believe that we can draw narratives and conclusions about what is going on in our modern lives and where our societies may be heading. Rather, like all good essays on modern human rights, we must warn of a dark future. The warning we wish to develop in this paper is that the transformative view of technology, as riddled as it is with its own internal challenges, poses significant risks not only to privacy, but to how we as societies deliberate about how we choose to live our lives.

Privacy and Technology as Evolving Concepts...

The ways we conceptualise and greet technology and innovation is worthy of greater study. In the 1990s, with the threat of expanded use of cryptography, governments argued that new technologies prevented lawful access to information. They also argued that new techniques of communication, such as digital telephony and mobile communications were not built to allow for lawful access to communications. Therefore, they advocated the need to regulate and control new technologies.

After the rise of national security concerns following the terrorist attacks on September 11, 2001, and other attacks around the world, however, the role of technology changed -it was now to become an enabler for greater surveillance, through the ability to collect more data such as our travel and communications information, new forms of data we didn't previously collect such as biometrics and DNA, identify new threats through the use of profiling and data mining, and peer into domains previously considered sacrosanct such as beneath our clothes [2]. Through significant investment, these technologies became dominant in debates, and the promotion of these technologies became a priority.

In the midst of this evolution, the framing of technology also begun to change and advertising-based business models became common-place. 'If you're not paying for the product, you are the product', the adage goes. With the emergence of free applications and social networking platforms, a perfect storm unveiled, and the anti-regulation rhetoric became mainstream both in the world of security-related technology and the sphere of private consumption and social media. Regulation came to be considered anti-free market and anti-innovation, and the pro-privacy advocates begun to be seen as acting against progress itself [9].

But while it is impossible to deny that technology has influenced privacy policy deliberation and debate, the view that technology is transformative and comes down from above to forever change our societies is caricaturesque and simplistic.

There is a clear need to go beyond totalitarian statements such as 'technology is bad', or 'technology is essential', or 'innovation can't be prevented'. We are well aware of the oddity of these claims because all parties in our debates use them. Just as privacy advocates argued that technology was essential to protecting rights in the 1990s, these same advocates can be painted as being anti-innovation today because of their calls for constraints and rules. Similarly, governments that saw technology as problematic in the 1990s are now quick to proclaim opponents as luddites if they resist new forms of data collection, or greater spending on large IT projects. Meanwhile, the businesses that demand unhindered innovation today are often seeking at the same time legal protections in intellectual property, or seeking rents from governments to permit access by building technologies to meet the interests of governments [10]. Rigid debates and understandings, therefore, are ill-suited for the necessary debate on technology, privacy and policy.

In the same way as there are divergent interests and positions within the policy stakeholders involved in the privacy debate, there are also varying conceptualisations of privacy in relation to technology [11][12]. In the context of information technologies, privacy usually stands for *information privacy*, a term that is quite useful in combining the privacy of personal communications with the privacy of data [13]. Information privacy is defined as the right of an individual to control the ways in which personal information is obtained, processed, distributed, shared, and used by any other entity [14] and so it incorporates the notion of 'control over information' as an underlying assumption of data protection legislation, which often assumes that control over the ways in which personal information is obtained, processed, distributed, shared and used by third parties is key in terms of public self-determination and empowerment [15].

However, this emphasis on control tends to get lost in broader understandings on how to embed privacy and rights in technology, or divorced from other important notions, such as trust and acceptability. Since the way people perceive and negotiate their own privacy is often determined by technological awareness, earlier beliefs about institutional settings and confidence in the institutions using the technology [16], it becomes increasingly clear that debates over privacy and technology need to go beyond rigid definitions to encompass changing social relations.

In this process, it is important to move away from the widespread recurrence to the trade-off approach in framing privacy and security issues, especially when it comes to technology. In public safety discourse, privacy is often discussed from a cost-benefit perspective, and the relationship between security and privacy is framed as a trade-off, a zero-sum game –we give up privacy in exchange for security. However, there is a growing body of academic work that questions the traditional definition of the trade-off between privacy and security as a useful way of looking at people's relation to technology and surveillances, as the trade-off approach undermines 'a number of ethical, social and political implications increasingly associated with the introduction of new surveillance-oriented security technologies' [16] such as how the storing, classifying, retrieving and matching of personal information promotes social sorting [17] and reinforces social, economic and cultural inequalities. The increasing reliance on technology-assisted profiling techniques to prevent terror and crime are also contributing significantly to the creation of a general climate of fear which may have serious consequences in terms of social cohesion and solidarity [18].

Another shortcoming of current conceptualisations of the relationship between privacy and technology is the difficulty to integrate, both legally and in engineering terms, the shifting nature of privacy. Cultural settings, personal attributes such as age and lifestyle, technological awareness, dependency, etc. can influence how privacy is perceived and understood by different cohorts or by the same person at different stages of their life or in different settings.

Given that privacy is not a static idea, but a changing anthropological feature, it should not and cannot be designed and embedded into technologies as an 'a priori' functionality alone. The link established by the literature between the evolving notions of private and public, legal protection from unwarranted intrusion and issues of control, trust, acceptability and empowerment point to the need to introduce flexibility as a key concept in technological development. If privacy is an evolving concept that is individually negotiated depending on contextual factors, the ability for users to have decision power and information over how the interface between private data and public data is negotiated by the devices they use or the surveillance technologies they are subject to emerges as a key arena. At this interface, sociological concerns, legal constraints and technological possibilities must establish a dialogue that is able to interact with the changing characteristics of the context of implementation.

... and the Implications for Policy-making

However, in the same way that current solutions to the technology/privacy dilemma, such as Privacy by Design (PbD) or Privacy-enhancing technologies (PETs) are still struggling to come up with engineering solutions to complex social concerns (see **Box 1**), the law is also finding it difficult to overcome the challenges linked to regulating surveillance –and as long as the law is not settled upon these concepts, we can't expect our technologies to draw the lines carefully. Even then, our techniques and technologies represent and implicate privacy and surveillance in drastically different ways. For example, a body-scanning technology that peers beneath our clothing can come in many forms -one that shows detailed body information, one that peers into cavities, one that shows only outlines, one that shows the data in real time in the booth, one with remote viewing, one with storage capabilities, one linked with identity. These can also be the characteristics within the same system implementation. Therefore, no two system implementations are designed equally when it comes to privacy.

These dynamics make it harder to actually deliberate around technology and society. 'Technology' is not a single artefact, just as the societal and policy institutions are complicated. This frustrates the rhetoric in debates -'internet spying is bad', 'CCTV reduces crime', 'Police need these powers to fight against pornographers', 'Government is acting like Big Brother', 'Google profiles every click you make', 'Facebook sells you to advertisers' are all commonly used in debates, but they are gross allusions to the simplicity of institutions and technologies. Privacy, surveillance, the technologies and the stakeholders all deserve better than this. But saying this isn't an attack on the simplifiers -it's a reprimand on how we all approach technology and policy.

When dealing with the strategies and need to influence policy, for instance, common actor-categorisations of 'business', 'advocates', and 'government' can be too raw. 'Advocates' are not some simple and coherent grouping -an advocacy 'group' that may have opposed government restrictions on peoples' rights to use cryptography to secure their communications will not necessarily oppose the greater use of profiling techniques by behavioural-targeting advertising companies. The conceptualisation of a 'group' or an 'advocate' of privacy varies widely too –sometimes they are sole individuals, sometimes they are large organisations with their own deliberative processes [19], and they may also exist within governments, and companies [5].

Similarly, 'governments' are not single minded institutions [20] –a ministry that seeks to deploy surveillance techniques may run into opposition from another ministry that seeks to promote innovation and openness, or with individuals and regulators that seek to protect human rights.

Finally, companies also consist of varying departments, objectives, and interests that remain in flux–in our experiences we have seen companies turn from being anti-privacy into pro-privacy, back into anti-privacy modes within short periods, and sometimes even displaying these stances simultaneously[2] .

This is not to say that the task is easy or that the cracks in the system will work on their own to make the debates relevant and the solutions pertinent and proportionate. It is hard to deny that we do not yet have adequate deliberative measures for modern policy-making where technology is involved.

When it comes to modern surveillance techniques that use highly sophisticated technologies, decision-makers are ill-equipped to understand the risks or advantages beyond simpler representations from opponents and proponents. Debates around identity cards and biometrics, DNA databases and communications surveillance are always filled with claims of super-effectiveness and super-invasiveness and claims that technologies will necessarily fail.

This points to the urgent need to articulate an informed public debate on the issues linked to technology, innovation and privacy–a debate that allows policy-makers and regulators to understand the social implications and reach of their decisions; politicians to avoid the temptation of technological determinism and 'acting out' and prioritize a deep understanding of the economic and legal consequences of their decisions; to technology developers to adapt their capacities to the expectations of users and citizens and the regulatory framework; and to the population in general to have tools to assess the possible implications of technological development and innovation for individual and collective rights and social cohesion.

Exploring New Conceptual Frameworks

When political institutions are on the leading edge of technology and policy-making, and particularly when invoking legal measures, it is common to reach to analogies, to look to the previous technology frames to identify what was once decided about those, and then try to apply that to the new. The debate then becomes one about which frame we wish to apply.

One of the earlier challenges of this type in the domain of privacy occurred in the early 1920s in the United States. The Supreme Court was asked to make a judgment in the case of Olmstead. Olmstead was a bootlegger, and his telephone communications had been intercepted by Federal law enforcement officials. He argued that this was in conflict with the Fourth amendment to the Constitution of the United States, which states that '*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*' Even though the term privacy is not mentioned in this passage, Olmstead believed that the interception of his telephone calls constituted an unwarranted search and seizure. As the constitution was written in a time pre-dating voice telecommunications, he adapted the constitutional statement to one where he equated his communications with this home, papers and effects. If the police were to seize his voice communications, this had to be equated to entering his home, seizing his papers and effects.

The Court disagreed with his equation. Justice Taft, for the Majority, Olmstead v. United States, U.S. Supreme Court 1928, wrote that "*The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment*"[3]. There was an interesting dissenting opinion from Justice Louis Brandeis, stating that when the Fourth and Fifth Amendments were adopted, "*the form that evil had theretofore taken*" had been necessarily simple. Before telecommunications, force and violence were the only means known to man by which a government could directly effect self-incrimination. Possession of a citizen's papers and other articles incident to his or her private life could only be secured by breaking and entry, but, Brandeis continued, "*Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet… The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.*"

The Olmstead case shows that there are always different frames at hand, and that the key resides in whose framing dominates the debates and deliberation. When the US Department of Homeland Security custom's agency began seizing laptops of travelers at the US Border, for instance, it argued it was merely acting in accordance with standard practices –but is a portable computing device the same as a piece of luggage? Or is the search of a laptop full of emails, company and personal files the equivalent of searching one's home? Similarly, it was recently uncovered that the Metropolitan Police in the UK were scanning the mobile phones of people who were arrested, and keeping the data indefinitely. In the age of 'dumb' phones, this would merely capture the information of who called who, but in the 'smart' phone era this is perhaps the equivalent of a laptop search, and in turn the search and seizure of information from the personal sphere –usually protected by law.

Often times, it is those who speak the loudest, with an agenda of their own, who come to dominate the language and the implications with their powerful narratives. The inability to jiggle with different frames, however, can stop us from taking account of developments that occur outside of our field of vision. In seeing technology as an ever-faithful companion to state surveillance, for instance, one might fail to notice how social networking, the internet and communications more generally are essential to the protection of human rights and democracy -as displayed to some extent in the Arab Spring. What emerges is the need to go beyond 'transformative' appraisals of technology, with their technological determinism, and the associated demands that social structures adapt to new techniques and technologies, to rather embrace an understanding of privacy and technology that begins by asking not 'what is technologically possible' but 'what kind of society we want to live in'.

Eight Perspectives on an Urgent Debate

The main challenge, left to the reader, is to ask how we may better make decisions as citizens, consumers, and participants in markets and democracies, as policy stakeholders and policy-makers. This edited volume is a contribution to such debates and challenges, by presenting a broad range of works that tackle the issue of privacy and technology from different angles and perspectives, and using cases that range from the public to the private sector, from online platforms and social networks to the offline realities of paying with a credit card, going through a body scanner at an airport or having your ID scanned to enter a night-club.

The contributions included in the following pages address questions related to the role of corporations in the shaping of the controversies that emerge around the issues at stake, people's and society's changing attitudes to privacy (in the specific case of online natives, for instance, or business models) or the relationship between privacy, technology and other forms of control in countries ranging from Brazil to Australia. A theme that runs throughout this special edition is the limits of current definitions and understandings of privacy, and of the regulatory tools that are meant to negotiate the relationship between fundamental rights and technological possibilities.

While many of the contributions address the issue of privacy and technology in the online sphere (looking at Google, Facebook and social networks in general), some of them translate the controversies to the offline world. In order to contribute to an understanding of the relationship between privacy and technology that resonates both online and offline (or away from the keyboard, as some would say), the contributions are organized in a way that mixes the approaches and forces the reader to travel between different regulatory frameworks, spaces and technologies.

In order to set the scene, the first contribution reviews key issues and concepts on privacy and surveillance technologies for both practitioners and advocates. By reviewing the current state of the debates on privacy (and asserting that it is far from dead) and putting it in relation with the processes, sites, modes and subjectivities of technology-mediated surveillance, ***Aaron Martin*** shows how complex is the emerging cartography of privacy and technology. In its first part, the article emphasizes that the emergence of social sorting, dataveillance and cyber-surveillance, to mention just a few of the practices that are giving shape to the field, demands that privacy is addressed from the perspective of *activities*. As a complex, changing and negotiated principle, privacy is therefore best captured *in action*. In the second part of the piece, the author addresses issues linked to the political economy of surveillance, resistance, regulation and Privacy-Enhancing Technologies (PETs) thus describing the different 'spaces' where the privacy and technology debate is taking place.

After Martin's thorough review of the issues at stake in relation to surveillance-enabled technologies, ***Gloria González-Fuster*** and ***Rocco Bellanova*** and capture similar issues (how the privacy and technology debate is taking shape) from a different perspective. The authors challenge of language, definition, and conceptualisations in policy deliberation when addressing issues related to privacy. They examine the tensions between the conceptualisation of European personal data protection "*as an autonomous legal notion and its envisioning as part of a wider privacy notion*." As Europe deliberates on its new legal frameworks for protecting personal data, there is a need to ask how this relates to the protection of privacy. They identify a confusion where 'personal data protection appears to be sometimes understood as an equivalent to privacy (then interpreted as 'informational privacy' or control over personal information), sometimes as an element of privacy (then portrayed as a wide right, not limited to the protection of what is 'private' in the sense of opposed to 'public') and sometimes as different from privacy (then potentially contracted to a mere protection of the 'private' as opposed to the 'public')'. This has implications for the eventual legal instruments and how they will become understood and applied in the future.

This special issue's third contribution is centered on how in the last 30 years surveillance-enabled technologies have been seen as a vital tool in the fight against crime and terrorism. By looking at the recent attempts to regulate detection technologies, ***Mathias Vermeulen*** suggests that current norms and guidelines are failing to understand what privacy is and how is violated, and the spirit of the legal protection of the right to privacy. He focuses on a recent decision by the European Court of Human Rights establishing that the safeguards developed for detection technologies are not applicable in the case of covert surveillance with GPS devices, thus giving 'location privacy' less protection than the privacy linked to 'behavior, opinions or feelings'. This decision shows how the debate on privacy and technology is taking shape, sometimes in ad-hoc ways and without a proper debate on the implications of specific decisions and understandings of the right to privacy in the context of emerging technologies.

By focusing on the deployment and functioning of ID scanners, databases, surveillance and crime prevention in Australia's night-time economy, ***Darren Palmer*** and ***Ian Warren*** depart from more theoretical, legal or conceptual understandings of the relationship between privacy and technology to identify how surveillance-enabled technologies permit function creep –their use for purposes other than the original intention- and how this interacts with the management of government services. Not only does this have implications for government departments as they grow dependent on surveillance technologies, but Palmer and Warren warn that there "*is little scope for privacy law to allow citizens to collectively challenge the growing function creep of new surveillance technologies employed by police, other government departments or private businesses.*" They are concerned that "*the political tendency to introduce and endorse these technologies without adequate public debate is arguably fuelled by the current legal exemption of crime under contemporary Australian privacy law*", and thus point to the need to better address the interaction between privacy, public and private bodies and security.

In the fifth contribution, on Google, security, the freedom of information, ***Cristina Blasi-Casagran*** and ***Eduard Blasi-Casagran*** tackle the dominating role Google has among search engines and internet services in general, and describe the development of new business forms made possible by new technological developments. These new business forms, however, pose numerous challenges to the right to privacy as they rely on the processing of large amounts of personal data in order to make a profit. Using Google as their main entry point, the authors describe three spaces of controversy –behavioural advertising, the right to be forgotten and the growing confusion around the use that public and private bodies give to the personal data they gather (echoing some of the points raised by Palmer and Warren). In their paper, Blasi and Blasi analyze in real time the debate on the conceptualization of the rights, duties and obligations of public administration, private bodies and citizens in the internet era.

Recovering some of the issues raised in the previous paper, ***Fernanda-Glória Bruno et al.*** highlight the importance of the industry dedicated to the processing and management of personal data and describe how it works and what its practices are. Through the study of behavioural-analysis techniques used in marketing and using cookies, the authors argue that just because we don't know about what is being done with our personal information, this should not be considered the new normal. They ask instead how a regulatory framework can catch up with the pace of innovation, particularly in the case of Brazil, where regulation has yet to emerge. They point out that one of the key challenges provided by surveillance technology policy debates is that unlike other forms of policy debates, we often do not know that we are subject to surveillance. As such, the traditional safeguards are hard to apply – "*opt-out options and user choice are hard to exert given the lack of transparency of such a context. Moreover, they cannot be taken as an easy way to get rid of the obligation of giving an adequate political response to the privacy problems posed by behavioral targeting practices. If current practices shrink the space for negotiation, it thus requires us to rescue the social value of privacy.*"

If Blasi and Blasi emphasize the need for regulation to incorporate the evolving elements that emerge in the debate around the right to privacy, ***Massimo Ragnedda*** approaches this same challenge from the point of view of the difficulties that 'digital natives' face when managing their privacy. In his field work with students in Sassari (Italy), the author addresses the impact of Social Network Services (SNS) on our lifestyles and ways of relating to one another, as well as the difficulties of controlling private corporations that base their profit model on the gathering and analysis of large amounts of personal information. The paper also deals with issues related to the perception of risk and of oneself both online and offline, showing how SNS users tend to combine a lax attitude toward their own privacy online with a degree of hiper-protectionism of their personal data offline. Analysing student's responses to questionnaires, Ragnedda paints a picture of unawareness and defenselessness that is having a profound effect in the development of the subject's personal identities and their perception of other people's rights, as shown by the fact that a little over 40% of the students in the study declared asking for permission before disclosing other people's personal information or images. The author thus shows the need to tackle the issue of privacy and social network use both prom the point of view of the protection of users and the understanding of the expectations and environment of 'digital natives'.

Going back to offline technologies, ***Joan Figueras-Tugas*** reminds us again that the controversies linked to technology, privacy and security are not exclusive to the online world, even though social media and social networks take a protagonist role in the study of the social impact of new technologies. In his paper on body scanners at airports, Figueras takes the debates put forward by the rest of the contributors to the management of civil aviation and critical infrastructures. He follows the policy debates that have taken place in Europe since full-body scanners were first introduced, in early 2010, and the first proposal for a common legal framework published by the European Commission in 2011. In the trial months, different scanners with different technologies were installed in many countries (the author describes in detail the cases of Great Britain, Finland, The Netherlands, Italy and Germany), and even though the EC proposal is a first step towards ho-

Currently the debate on the relationship between privacy and technology is dominated by two main paradigms which in theory are complementary but in practice present very different understandings of engineering and technology. While Privacy by Design (PbD) is based on a list of principles that have been adapted by several private companies as a set of general recommendations to take into account in product development, Privacy-Enhancing Technologies (PETs) constitute specific technological solutions based on control, transparency, data minimization and anonymity.

PbD: Privacy-by-Design

The concept was developed in the 90s by Ann Cavoukian, Ontario's Information & Privacy Commissioner, and refers to "the philosophy of embedding privacy proactively into technology itself – making it the default" (Cavoukian 2009). The proposal is structured around a set of "foundational principles": *1.* PbD anticipates and prevents privacy invasive events *before* they happen. (*Proactive* not *Reactive*/*Preventative* not *Remedial*); *2.* No action is required on the part of the individual to protect their privacy — it is built into the system, *by default* (Privacy as the *Default Setting*); *3.* Privacy is integral to the system, without diminishing functionality (Privacy *Embedded* into Design); *4. PbD* avoids the pretence of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both (Full Functionality/*Positive-Sum*, not Zero-Sum); *5.* PbD ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion (End-to-End Security/*Full Lifecycle Protection*); *6.* PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification (*Visibility* and *Transparency*/Keep it *Open*); *7.* Above all, PbD requires system architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options (*Respect* for User Privacy/Keep it *User-Centric*).

Privacy-Enhancing Technologies (PETs)

Privacy-Enhancing Technologies generally refers to any tool or mechanism integrated in technological devices designed to increase the anonymizing capabilities or control functions over personal data, while at the same time avoiding the loss of the functionality of the information system (van Blarkom et al. 2003). PETs are thus technical means to increase people's control over their personal information, minimising the data disclosed to private companies and the state, making privacy-invasive data-processing more transparent, and anonymizing communications between parties. Therefore, PETs are not a set of general principles, but specific technologies and solutions such as encryption software, anonymizers, and browser extensions that provide granular data controls. Real-world examples of successful PETs include tools such as Tor (www.torproject.org), which provides a secure means to surf the web and communicate privately, and Ghostery (www.ghostery.com), a browser plug-in that shows the tracking tools embedded on web pages (Martin 2012). While there is consensus on the need to generalize such technological solutions, to date only a small minority of developers and users are familiar with and use PETs.

Box 1. On the Relationship between Privacy and Technology: Privacy-by-Design and Privacy-Enhancing Technologies.

mogenization and the development of a rights-based framework, the author identifies different unanswered questions that point to the need to rethink the role of surveillance technologies in critical infrastructures by emphasizing the importance of respecting fundamental rights and developing a broad understanding of security.

One of the issues that all contributors point to is the difficult relationship between the legal and normative conceptualization of the right to privacy and the realities of an evolving society and changing technology, what emerges is thus a scenario that requires a proper, informed debate, but also better technological solutions, adapted to the political and social needs (and not the other way around), accountable and open to citizens' control.

References

[1] C. Sunstein. *Republic.com 2.0*. Princeton University Press, 2009.
[2] D. Lyon. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.
[3] DJ. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):477-564, 2006.
[4] Christena Nippert-Eng. *Islands of privacy*. Chicago: University of Chicago Press, 2010.
[5] K. Bamberger, D. Mulligan. Privacy on the Books and on the Ground. *Stanford Law Review, Vol. 63(1)*: 247-316, 2011.
[6] A. Etzioni. *Limits of Privacy*. New York: Basic Books, 2000.
[7] S. Baker. *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism*. Stanford: Hoover Institution Press, 2010.
[8] R. Posner. *Not a Suicide Pact: the constitution in a time of national emergency*. Oxford: Oxford University Press, 2006.
[9] J. Jarvis. *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live*. New York: Simon & Schuster, 2011.
[10] C. Soghoian. An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government. *Minnesota Journal of Law, Science & Technology. 2011*;12(1):191-237.
[11] L. Introna. Privacy and the Computer: Why we Need Privacy in the Information Society. *Metaphilosophy, 28(3)*: 259-275, 1997.
[12] H. Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press, 2010 (Spanish Translation Mexico City: Océano, 2011).
[13] R. Clarke. Make Privacy a Strategic Factor — The Why and the How. *Cutter IT Journal, 19*(11), 2006. <http://www.rogerclarke.com/DV/APBD-0609.html>.
[14] A. Acquisti, S. Gritzalis, C. Lambrinoudakis, S. De Capitani di Vimercati (Eds.). *Digital privacy: theory, technologies, and practices*. New York: Auerbach Publications, 2008..
[15] E.A. Whitley. Informational privacy, consent and the "control" of personal data. *Information Security Technical Report, 14*(3), 154-159, 2009.
[16] V. Pavone, Degli Esposti. Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. *Public Understanding of Science*, 21(5): 556-572, 2012.
[17] D. Lyon. *Surveillance as social sorting: privacy, risk, and digital discrimination*. London: Routledge, 2003.
[18] OSI. *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*. New York: Open Society Institute, 2009.
[19] C. Bennett. *The Privacy Advocates: Resisting the Spread of Surveillance*, Massachussets: MIT Press, 2008.
[20] E.A. Whitley, G. Hosein. *Global Identity Policy*. London: Palgrave MacMillan, 2009.

Notes

[1] This sentence has been attributed to Mark Zuckerberg, founder of Facebook, but it has been echoed by many in the business of data mining and analysis, and is shared more broadly by those who believe that only those who have something to hide should fear the death of privacy.

[2] This is the case of Google. See, for instance, <http://arstechnica.com/business/2012/04/google-releases-full-details-of-fcc-investigation-into-street-view-wifi-snooping/>.

[3] Olmstead v. United States, 277 U.S. 438 (1928).

CLEI

Centro Latinoamericano de Estudios en Informática

CLEI --- www.clei.org --- es una asociación sin fines de lucro con casi 40 años de existencia, y que reúne a más de 100 universidades, centros de investigación y asociaciones de profesionales latinoamericanas, y algunas extra-territoriales (españolas y estadounidenses) interesadas en promover la investigación y docencia en Informática.

CLEI invita anualmente a presentar trabajos que reporten resultados de investigación y/o experiencia originales durante su **Conferencia Latinoamericana en Informática (CLEI).** En la conferencia, que se realiza típicamente en octubre, participan aprox. 1000 personas, y se reciben para sus simposios, más de 500 artículos en castellano, inglés y portugués, de los cuales el 33% son aceptados.

A partir del 2012, las memorias de la CLEI son publicadas en **IEEE Xplore**. Además, números especiales del **CLEI Electronic Journal** son dedicados a trabajos seleccionados de esta conferencia.

Simposios CLEI

- Simposio Latinoamericano de Ingeniería del Software
- Simposio Latinoamericano de Informática y Sociedad
- Simposio Latinoamericano de Investigación de Operaciones e Inteligencia Artificial
- Simposio Latinoamericano de Infraestructura, Hardware y Software
- Simposio Latinoamericano de Sistemas Innovadores de Datos
- Simposio Latinoamericano de Teoría Computacional
- Simposio Latinoamericano de Computación Gráfica, Realidad Virtual y Procesamiento de Imágenes

Eventos Asociados (realizados en paralelo anual o bienalmente)

- Congreso Iberoamericano de Educación Superior en Computación (CIESC)
- Concurso Latinoamericano de Tesis de Maestría (CLTM)
- Congreso de la Mujer Latinoamericana en la Computación (LAWCC)
- Simposio de Historia de la Informática en América Latina y el. Caribe (SHIALC)
- Latin America Networking Conference (LANC)
- Workshop en Nomenclatura y Acreditación en Programas de Computación

clei·electronic·journal

Aaron Martin
London School of Economics and Political Science

<A.K.Martin@lse.ac.uk>

Privacy and Surveillance Primer

Abstract: *Activists, scholars, and policy makers are increasingly recognizing that excessive surveillance (very often enabled by new forms of information and communications technology ICT) can be harmful to society. But in order to understand how these surveillance developments may detriment the fostering of healthy, open, and democratic societies, we must first know where to look for a conceptual basis, and even more importantly, what to look for once we're there. This article therefore reviews key issues and concepts on privacy and surveillance for practitioners and advocates who are eager to understand and engage these multifaceted topics, particularly as debates about the benefits and risks of disclosing and sharing our data become more dynamic and significant.*

Keywords*: Conceptual Overview, Privacy, Surveillance, Technology.*

Author

Aaron Martin has researched privacy and surveillance topics since 2004, most recently as a technology policy analyst at both the OECD and European Commission's Joint Research Centre. In 2011 he earned a PhD in biometrics policy from the London School of Economics while also working as a privacy analyst at the Vodafone Group, where he focused on the areas of communications surveillance and location privacy. He also regularly collaborates with Privacy International, a civil society organization that defends the right to privacy across the world. These experiences provide him with a unique perspective spanning the worlds of research, policy, industry, and civil society from which to survey the current lay of the privacy and surveillance landscape.

1. Introduction

In business and technology circles it's in vogue to declare the death of privacy. Mark Zuckerburg proclaimed it. So did Eric Schmidt. The incredible popularity of social networking sites, free apps, and online services bears testament to the vast changes taking place. Even simple words like "free" don't mean what they once did. Using a free platform is supposedly now equivalent to giving consent for personal information to be collected, manipulated, and sold. "If you aren't paying for it, *you're the product*," or so they say. In this new, wondrous digital economy, personal data is hard currency. The platforms have become such an integral part of society that coughing up a name, an e-mail address or some browser history seems a small price to pay in exchange for access to the mainstream. This is exactly the kind of voluntary disclosure Zuckerburg talks about, but it isn't always voluntary and it definitely isn't "free" in the traditional political sense of the term.

The reality is, of course, much more complicated. The arguments that Zuckerburg and others make are naïve perhaps intentionally naïve. Privacy isn't dead and it will likely never die, even as new data-intensive business models proliferate and surveillance becomes less expensive, more effective, and far more pervasive. Who governs and makes use of personal information is what's most at stake: Facebook wants to govern rules for sharing, but more importantly wants dominion over vast amounts of information about what we do and who we know; Google competes to know more about what we're seeking and where we're going online. And even still, focusing on those two institutions, as so many stories do, misses the larger points about the rapidly evolving social and technological environments in which we're constantly struggling to appreciate the implications of new developments.

We need to understand how these developments are detrimental to the fostering of healthy, open societies. Before we can make a concerted effort to harness these technologies for the benefit of open societies, we must first know where to look and what to look for. For this reason, a review of key issues in privacy and surveillance is much needed, and I'll attempt to provide that here.

2. Privacy as a Problematic

Privacy is one of society's most contentious concepts. Scholars love to quibble about the definition of the term. There's some debate as to whether privacy is an exclusively Western construct that makes little or no sense elsewhere. Culturally relativistic arguments apply equally to many issues, but the appeal to cultural relativism is also one of power and opportunity: we rarely entertain debates about copyright being culturally relative. Different cultures may define what's private in dissimilar ways. Often the problem is finding the appropriate language to discuss privacy-related matters with those of a different culture, society or community.

Communitarians such as Amitai Etzioni argue that privacy rights must be balanced with the common good that individual privacy rights cannot be absolute [1].

Proponents of communitarianism offer a set of criteria for balancing the right of the individual against the good of society, including assessing privacy-friendly alternatives, aiming for minimal intrusion into one's private life, and reducing undesirable side-effects. These principles are reflected in many international statements on privacy and human rights.

There's also an interesting feminist critique that challenges the historical concept of privacy. Siegel notes that men have historically used privacy claims to protect their home ('man is the master of his domain'), thereby linking privacy with domestic harmony in such a way that legitimated marital abuse. "*This right of privacy is a right of men 'to be let alone' to oppress women one at a time*" [2].

The modern challenge is to consider how these debates are reflected in our technological societies and changing economies. Sure, privacy must be balanced and the criterion may differ across legal systems but how is this negotiated when we consider the design of new technological infrastructures? Do we instill the 'balance' into our designs, perhaps by ensuring that all computers have backdoor vulnerabilities for police to gain access? Similarly, technology is changing the modern family environment and there are new challenges about privacy that we must consider with regards to relationships and children. But protections could be democratized rather than only be available to the dominant forces within societies.

3. Framing the Debate

While these critiques are important and force us to think critically about the value of privacy, none of them offers a total rebuttal [3].

An essential systematic treatment of the concept comes from the legal scholar Daniel Solove, who provides some practical clarity in his *Taxonomy of Privacy* [4]. The taxonomy captures the various facets of privacy without dismembering or disunifying it. Solove moves past theoretical disputes (is privacy a human right, legal right, consumer right, cultural construct, etc.?) to explore more practical evidence of privacy in action: *activities* that pose privacy problems. He identifies four main categories (collection, processing, dissemination, and invasion) unpacking each

“Much has been said about ICT's democratizing capacity. Yet less remarked upon is how the Internet and related technologies democratize surveillance as well”

in depth, and providing a solid framework to organize debate on privacy and surveillance.

This debate is everything. If privacy is a negotiated right, one that must be balanced against other rights and for national security, or for economic progress, we must have a debate about how the lines are drawn. The lack of debate is what leads to the greatest incursions. The inability to revisit older debates may be an inhibitor to progress and innovation. Therefore the promising aspect about privacy is that in many key places the debate is ongoing, and getting louder and stronger. That, if anything, is a good thing.

4. Processes of Surveillance: Categorization and Social Sorting

Privacy isn't just an individual condition. On a macro scale, sociologists of surveillance such as Oscar Gandy [5] and David Lyon [6] have illuminated different ways in which information technology operates to discriminate between people and groups of people, for the purpose of controlling them.

Surveillance is a layered process. Before surveillance comes *categorization*, which is actually a two-step event: label first, then classify. We do this all the time: male and female, credit-worthy and sub-prime, 'safe' traveler and potential threat, etc.

There's nothing inherently bad about categorization. As Michel Foucault made clear in *The Birth of the Clinic* [7], categorization is a key component of human knowledge and an indispensible aspect of our power to change our reality. First we distinguish between 'healthy' and 'sick', with obvious practical benefits. Then we distinguish between people with eye problems and people with foot problems, for example, and so it goes down the line. By grouping together like patients and removing outliers, we learn more about their condition and through that knowledge we gain the power to change it. Of course, categorization has its dark side too. Someone branded a 'criminal', is associated with other criminals, and may continue to be associated with that group even if officially exonerated.

Categorization is important because it facilitates *social sorting*. Once subjects are labeled and bundled, they can be sorted, managed, and potentially controlled, which could have the beneficial impacts Foucault observed in the clinic but could also degrade fundamental rights and freedoms like movement and speech, and even life chances. Scholars concern themselves with the detrimental aspects of surveillance, but deserved scrutiny shouldn't negate the potential upside. This isn't about a trade-off; it's simply to say that when these practices aren't transparent or go unquestioned, the potential for negative outcomes increases. Privacy advocates continually expose and dissect systems of surveillance and categorization to understand their logics, operations, and social consequences to find the border between their beneficial and deleterious applications.

5. Sites of Surveillance

Mapping this border is more like mapping galaxies than distinguishing between rooms in a house: knowing where to look is a precondition of both, but a much more severe challenge in the first instance than the latter. Consequently, discovering *where* surveillance happens is becoming increasingly important. There's a long and growing list of sites of surveillance, regularly padded by advancements in technology and new policies that require increased information collection.

Many of these sites, like airport security checkpoints, are familiar and normal to us, though the underlying politics involved is less clear, as Mark Salter's work shows [8].

Some sites are less obvious. Our bodies are regularly sites of surveillance, as biometric devices and body-scanners work to categorize us based on our physical characteristics. Workplace surveillance is also a commonplace (e.g., monitoring of Internet activity) and schools are increasingly sites for surveillance (through video recording, electronic attendance tracking, etc.), as Torin Monahan and colleagues have shown [9].

Surveillance in public places is becoming the norm in our cities, especially as the technology to monitor these spaces gets cheaper and easier to use. During protests and large gatherings public surveillance is often intensified for crowd control and law enforcement purposes, such as during the Occupy movements. Identifying the difference between public and private spaces and the according rights to individuals has long been controversial, but new borders in our lives and the new spaces we create give rise to new rules and domains.

Despite its prevalence, surveillance isn't equally distributed throughout society. Some groups are easier to monitor than others. For example, John Gilliom has documented how the poor (he studied low-income Appalachian mothers) are disproportionately subject to state monitoring [10]. We can all appreciate the state's public duty to prevent benefit fraud and other undesirable actions, but we cannot lose sight of the potential for economic and political disenfranchisement that can result from heightened surveillance. We must therefore critically examine how the sites of surveillance are distributed to see how this affects the potential for an open and equitable society.

Online monitoring (or 'cyber-surveillance') provides an interesting twist to the idea of 'spaces' for surveillance. The extent to which cyber-space is actually a space is debatable [11], but the fact remains that surveillance is rampant online.

Both the Internet and mobile phone networks lend themselves to extensive information collection and tracking. Online surveillance was primarily commercial for many years, driven mostly by the desire to restrict access to content based on user location, and to deliver advertising. Recently however, political surveillance has intensified online, with the Arab Spring being a recen and powerful example. Dissident activities were organized online and threatened governments tried desperately to identify dissidents.

Cyber-surveillance also alters the socio-economic dynamics of privacy. Gilliom's welfare recipients were disproportionally watched by state agencies but the economies of scale for surveillance online and over mobile phone networks make it very easy to identify, categorize, and discriminate everyone that's connected. Much has been said about ICT´s democratizing capacity. Yet less remarked upon is how the Internet and related technologies democratize surveillance as well.

6. Modes of Surveillance

The *how* of surveillance is likewise complex. These are the various modes of surveillance.

When asked about surveillance, most of us think of visual monitoring. Orwell's Big Brother in *1984* was always *watching*, and that association has stuck. While visual monitoring is no doubt an important form of surveillance, it isn't the only one we ought to be concerned about.

Now what's observable need not be visual. '*Dataveillance*' is a rising challenge. Roger

> "The fact that all our actions in today's society generate data about that action, or interaction, is grist for the mill of dataveillance"

Clarke coined the term to depict "*the systematic monitoring of people's actions or communications through the application of information technology*" [12]. The fact that all our actions in today's society generate data about that action, or interaction, is grist for the mill of *dataveillance*. And this emergent data may be more telling than the activity itself. A lone CCTV camera may capture your location at a particular time, and contents may disclose what you choose to share, but records of your communications potentially reveal a range of sensitive details about your life (who you speak with, when, possibly where, and all over an extended period of time[13]), to anybody that can access them.

Location surveillance [14] is also becoming more prominent. Modern mobile phones are a good example of a location surveillance technology. Following revelations of the surreptitious tracking of users' location [15], this form of surveillance has become a major policy concern (more below). Scholars are just beginning to engage the privacy aspects of location tracking, which goes to show how fast-moving these issues are.

Biometrics automatically identify or verify people based on features of their bodies. The technologies and techniques for biometrics include facial recognition, iris scanning, digital fingerprinting, and DNA profiling, to name a few.

In *Our Biometric Future*, Kelly Gates explains why facial recognition technologies were deemed a solution to the problem of international terrorism following 9/11, and explores what had to be neglected or glossed over about the technology for it to be seen as an appropriate security solution to the complex and multi-faceted challenges of combating terrorism [16]. The commonly held belief that our true identities are contained in our bodies means that this form of surveillance is likely to continue expanding.

Common beliefs aside, it is simple fact that none of these modes offers perfect information about a person. Each only permits a partial and limited understanding of our identities, relationships, whereabouts, communications, and so forth, depending on what information is collected and how accurately it may be in the form in which it's obtained. Still, the organizations and industries driving new surveillance innovations strive to reduce these limitations, with the ultimate (but impossible) aim of achieving perfect, ubiquitous, all-knowing surveillance.

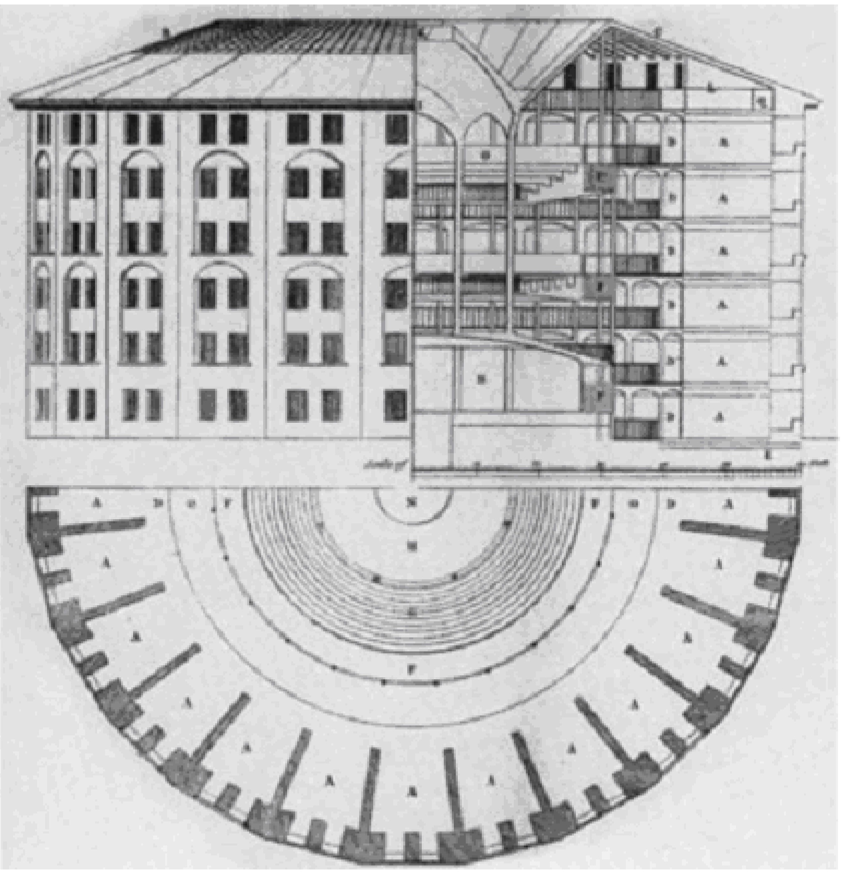


Figure 1. Jeremy Bentham's Panopticon

7. Subjectivities of Surveillance

Nonetheless, surveillance doesn't need to be perfect to be effective. Even imperfect surveillance can be a tool of social control because it tends to result in self-censorship and behavioral inhibition. This is one of the most important ideas on surveillance, first intimated by Jeremy Bentham and later developed by Foucault.

Bentham's Panopticon was a prison designed such that a guard could watch over all the inmates without them knowing whether or not they're being watched (see **Figure 1**). The mere possibility of being watched was thought to be sufficient to condition good behavior.

In the Panopticon, it isn't that those with nothing to hide have nothing to fear, but rather that the prisoners have everything to fear because they have no way to hide. Therefore, they regulate their behavior on their own, creating a normalized society without physical coercion. In *Discipline and Punish: The Birth of the Prison,* Foucault expanded Bentham's principal to all of society, which he thought disciplinary by nature. For Foucault, it isn't just prisons that normalize our behavior, but nearly all institutions [17]. The *mere possibility* of being watched is thus enough to modify behavior. As dissident Libyan journalist, Khaled Mehiri, remarked following the fall of Gaddafi: "*Surveillance alone is enough to terrorize people*" [18].

8. Political Economies of Surveillance

Again and again, we've seen private companies pop up as key drivers of innovations in surveillance and privacy. The political economies of surveillance are thus worthy of examination: Which business models require the extensive collection of personal information and how do these business models regard privacy? Is there a military or state security relationship to the means and motivations of surveillance? Which companies manufacture and sell surveillance software and equipment? This list goes on.

The case of surveillance drones [19] provides a rich example of the issues at play. Unmanned aerial vehicles were originally designed by the

> “The overarching point [of sousveillance] is to challenge the power dynamic inherent in surveillance to force transparency on organizations that conduct it”

U.S. military for battlefield reconnaissance. However, they have since been deployed in other contexts, such as along the Mexican and Canadian borders [20]. And even British police have expressed interest in using them domestically, to monitor drivers, protestors, and fly-tippers [21].

This phenomenon (known as ‘mission creep’ in the literature [22]) is the process by which technologies adopted for one aim are later repurposed to attain other policy goals.

Surveillance technology companies often operate and trade in secret; it has been difficult to discern the scale of the industry and the types of technology offered to law enforcement and intelligence agencies, making rigorous scholarly research in this area difficult. However, investigators and activists have begun to penetrate the secret conferences and venues in which these deals are made, and have subsequently begun to expose the trade. Much work remains to be done before this shadowy industry and its operations are understood.

9. Regulation and Governance

The regulation and governance of privacy and surveillance is hardly uniform [23]. Many countries offer constitutional privacy guarantees. Some don’t. Many countries have laws to regulate state and commercial collection and use of personal data. Others don’t [24].

Some jurisdictions observe laws regulating government access to certain types of communications data, as well as regulations for ‘lawful interception’: the circumstances under which it is legally permissible to intercept communications. Specific laws may also regulate specific types of data (e.g., health, financial or biometric information).

One problem with privacy and surveillance laws is that they’re often obsolete soon after they come into effect, as technology and innovation are so fast-moving. Even where relevant laws exist, they sometimes go unenforced. Enforcement typically requires a privacy, data protection or surveillance oversight commissioner to patrol the beat, and some countries (even those with privacy laws) don’t have such authorities in place. Where these agencies do exist, they’re often under-resourced or ineffective.

Many jurisdictions are responding to calls for privacy legislation, but privacy advocates must beware of so-called policy laundering a phenomenon that Gus Hosein has examined in depth [25]. Countries without national policies or regulations for protecting privacy or limiting surveillance powers sometimes replicate bad or ineffective laws from other jurisdictions, thereby replicated their (in)effects. Another opportunity for advocates involves fighting for stronger constitutional protections for privacy, which will provide a safeguard when unambitious or ineffective laws are put in place.

10. Resistance

Among the most creative ideas on resistance to surveillance is the concept of *sousveillance* proposed by Steve Mann [26]. *Sousveillance* inverts surveillance to fix the gaze upon the organizations that are normally involved in monitoring subjects. The overarching point is to challenge the power dynamic inherent in surveillance to force transparency on organizations that conduct it. A popular manifestation of *sousveillance* is citizen use of camera-enabled mobile phones to capture police brutality, such as during the 2009 BART police shooting of Oscar Grant in Oakland, California.

Another interesting resistance project involves ‘hacking’ facial detection systems by using makeup and accessories to prevent computer algorithms from detecting one’s visage. Adam Harvey discovered that facial detection systems can be confused by applying makeup on certain parts of the face (see **Figure 2**) [27]. By distorting our appearance, we regain the ability resist surveillance, and protect our privacy, if we so choose.

My colleagues and I have explored the networks of resistance that emerge to surveillance projects. Whereas the majority of the academic literature on surveillance is focused on resistance relations between the watcher and the watched, we look at different ways of understanding the *who* and *how* of resistance to elaborate a multi-actor framework to better understand the complex resistance relationships that arise in local contexts [28].

11. Designing Privacy Technologies

Harvey’s project may be categorized as a ‘privacy-protecting’ technology project in that it aims to use tools (in this case, non-information technologies like makeup and eyeglasses) to impede facial detection. In general, privacy-protecting or privacy-enhancing technologies (PETs) provide a technical means to resist surveillance by increasing people’s control over their personal information, minimizing the personal data disclosed to private companies and the state, making privacy-invasive data processing more transparent, and anonymizing communications between parties.

In building their tools, designers of PETs are actively contesting and resisting the politics and values that Nissenbaum and Howe argue are embodied by systems of surveillance [29].

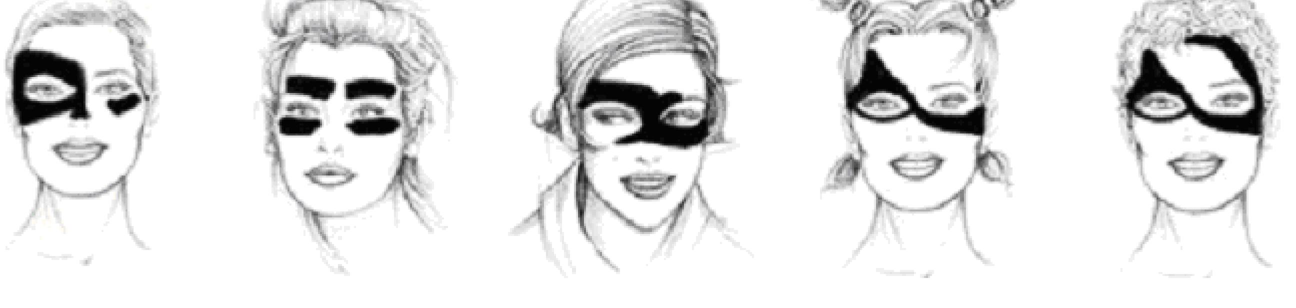


Figure 2. Low-tech Resistance to Facial Detection

> "The widespread diffusion of PETs would mark a major milestone in the advancement of privacy, but to date only a small minority of users has deployed them"

Real-world examples of successful PETs include tools such as Tor, which provides a secure means to surf the web and communicate privately, and Ghostery, a browser plug-in that shows the tracking tags, web bugs, pixels and beacons that are embedded in web pages. The widespread diffusion of PETs would mark a major milestone in the advancement of privacy, but to date only a small minority of users has deployed them; there's a high chance that you don't use them, and it's almost certain that grandma doesn't.

So the real challenge is to get them built into the infrastructure. Why can't the principles behind Tor be built into routers? Or the privacy and identity protecting principles [30] underlying Kim Cameron's Laws of Identity [31] be built into national identification cards? It could be due to the complexity of these techniques, or because there's a commercial and national security interest in ensuring systems that divide, identify, and reveal.

12. Identity, Pseudonymity, and Anonymity

One of the major privacy battles is the ongoing fight over identity policies online. For years it was possible to use the Internet anonymously, but the rise in trolling online, social anxieties about pedophiles luring and grooming children in chat rooms, and exaggerated fears about terrorists using the Internet to plan attacks have resulted in a push to force users to be traceable and identifiable online at all times.

From this belief emerged the so-called *nymwars.* On one side are online service providers, social networking sites, and even video gaming sites like Blizzard (makers of World of Warcraft [32]) that insist that people use their 'real' names on sites such as Google+. On the other side are academics, advocates, and activists who argue that there are many legitimate reasons for people to reserve the right to remain anonymous or to use pseudonyms online [33], such as political dissidents or anyone who faces analogue consequences for acceptable digital behavior. The good thing is, these are debates that academics have been engaging for years now. The list of recommended readings is extensive, but for starters I suggest the *Lessons from the Identity Trail* [34] edited volume and Whitley and Hosein's *Global Challenges for Identity Policies* [35], which explores how the odd couple of politics and technology is sometimes forcibly wedded to address the complex challenges of identity policy.

13. Targeting, Tracking and Mobility

Another area in much need of engagement and advocacy is online targeting and tracking. The use of tracking technologies like cookies is fairly normal online. They can be innocuous, but as free services proliferate online more and more sites and applications are relying on tracking-dependent advertising revenue. These companies collect lots of information about users in order to be able to more accurately target advertisements. Users who are uncomfortable with being tracked may try to limit the number of cookies that are installed on their computers, but advertising networks have become more aggressive in their practices by relying on new techniques such as Flash-based cookies [36] and other methods [37] for covert but persistent tracking.

In the U.S. and elsewhere, there have been calls to introduce legislation prohibiting companies from tracking people online without consent but it remains to be seen what technologies would support these policies and how effectively these provisions could be enforced. This is a complex ecosystem, in which it is difficult to exercise total control over personal data (such as location). There are numerous actors involved in collecting and processing information and as it stands it's difficult to discern where our data is flowing and how it's being used.

Still, both online targeting and tracking and mobile privacy present exciting opportunities for activists to get involved in designing technologies (such as visualization tools to increase transparency around online surveillance practices, or through secure communications tools such as what Whisper Systems has developed for Android phones), or by working to improve policy and regulation in this space.

The great challenge is that as the Internet and mobile phone systems become increasingly structured, with necessary intermediaries (ISPs), new intermediaries (hardware providers, operating system developers), and services (applications, browsers, platforms), the emerging fragmented solutions will be ultimately unsuccessful.

14. What's Missing?

Some very interesting research areas are inevitably missing from the above discussion. Surveillance labor is one: What's the actual practice of monitoring video surveillance feeds like and what role do things like emotions [38] and stress [39] play in the job?

Surveillance methodology is another interesting avenue: How can we measure surveillance, both quantitatively and qualitatively, in order to understand whether or not it's intensifying, and if so, how these changes are occurring? Kevin Haggerty has looked at these methodological conundrums [40].

The histories of different surveillance technologies also merit greater exploration. Simon Cole's historical exposition of fingerprinting methods in forensics serves as a strong example of this kind of research. He shows how the taken-for-granted idea that our fingerprints are unique (and thus capable of individually identifying people) is actually an epistemologically complex artifact [41].

And what about surveillance failures? All too often we fixate on successful surveillance policies and systems, but we tend to forget all the projects that are abandoned, fizzle or fail. There's a long list of surveillance technology that didn't make it (remember Total Information Awareness [42])? Why are such projects unsuccessful, and how are some apparently dead projects resuscitated and then incorporated into new initiatives (e.g., parts of Total Information Awareness still live on [43])?

Acknowledgements

This primer was funded by a grant from the Information Program of the Open Society Foundations, with intellectual contributions from Daniel Bernhard, Becky Hogge and Gus Hosein.

References

[1] **A. Etzioni.** *The Limits Of Privacy*. New York: Basic Books, 1999.

[2] **R. B. Siegel.** "The Rule of Love": Wife Beating as Prerogative and Privacy. *The Yale Law Journal,* 150(8): pp. 2117-2207, 1996.

[3] **S. T. Margulis.** On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues*, 59(2): pp. 411-429, 2003.

[4] **D. J. Solove.** A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3): pp. 477-564, 2006.

[5] **O. H. Gandy.** *Coming to Terms With Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Burlington: Ashgate, 2009.

[6] **D. Lyon.** *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003.

[7] **M. Foucault.** *The Birth of the Clinic: An Archeology of Medical Perception*. New York: Vintage, 1973.

[8] **M. B. Salter (ed.).** *Politics at the Airport.* Minneapolis: University of Minnesota Press, 2008.

[9] **T. Monahan, R. D. Torres (eds.).** *Schools Under Surveillance: Cultures of Control in Public Education*. New Jersey: Rutgers University Press, 2009.

[10] **J. Gilliom.** *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press, 2001.

[11] **M. Dodge, R. Kitchin.** *Mapping Cyberspace*. London: Routledge, 2000.

[12] **R. Clarke.** Information Technology and Dataveillance. *Communications of the ACM*, 31(5): pp. 498-512. 1998.

[13] **A. Escudero-Pascual, I. Hosein.** Questioning lawful access to traffic data. *Communications of the ACM*, 47(3): pp. 77-82, 2004.

[14] **D. Kravets.** Feds Seek Unfettered GPS Surveillance Power as Location-Tracking Flourishes. *Threat Level*, 7 November 2011: <http://www.wired.com/threatlevel/2011/11/gps-tracking-flourishes/all/1>.

[15] **B. X. Chen, M. Isaac.** Why You Should Care About the iPhone Location-Tracking Issue. *Gadget Lab*, 22 April 2011: <http://www.wired.com/gadgetlab/2011/04/iphone-location>.

[16] **K. A. Gates.** *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* New York: New York University Press, 2011.

[17] **M. Foucault.** *Discipline & Punish: The Birth of the Prison*. New York: Vintage, 1979.

[18] **M. Coker, P. Sonne.** Life Under the Gaze of Gadhafi's Spies. *Wall Street Journal.* 14 December 2011: <http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html>.

[19] **M. R. Calo.** The Drone as Privacy Catalyst. *Stanford Law Review Online*, 64: pp. 29-33, 2011.

[20] **J. Rayfield.** One Nation Under The Drone: The Rising Number Of UAVs In American Skies. *TPM Muckraker*, 22 December 2011: <http://tpmmuckraker.talkingpointsmemo.com/2011/12/one_nation_under_the_drone.php>.

[21] **P. Lewis.** CCTV in the sky: police plan to use military-style spy drones. *The Guardian*, 23 January 2010: <http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones>.

[22] **T. Monahan, N. A. Palmer.** The Emerging Politics of DHS Fusion Centers. *Security Dialogue*, 40(6): pp. 617-636, 2009.

[23] **C. J. Bennett, C. D. Raab.** *The Governance of Privacy: Policy Instruments in Global Perspective*. Burlington: Ashgate, 2003.

[24] **D. Banisar.** *National Comprehensive Data Protection/Privacy Laws and Bills 2012 Map*, 2012: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416>.

[25] **I. Hosein.** The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. *The Information Society*, 20(3): pp. 187-199, 2004.

[26] **S. Mann, J. Nolan, B. Wellman.** Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society*, 1(3): pp. 331-355, 2003.

[27] **D. Goodin.** Reverse-engineering artist busts face detection tech. *The Register,* 22 April 2010: <http://www.theregister.co.uk/2010/04/22/face_detection_hacking>.

[28] **A. K. Martin, R. E. Van Brakel, D. J. Bernhard.** Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*, 6(3): pp. 213-232, 2009.

[29] **D. C. Howe, H. Nissenbaum.** TrackMeNot: Resisting Surveillance in Web Search. In *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press, pp. 417-436, 2009.

[30] **S. A. Brands.** *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge: MIT Press, 2000.

[31] **K. Cameron.** *The Laws of Identity*, 2005: <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>.

[32] **BBC News.** World of Warcraft maker to end anonymous forum logins. *British Broadcasting Corporation,* 7 July 2010: <http://www.bbc.co.uk/news/10543100>.

[33] **J. C. York.** A Case for Pseudonyms. *Electronic Frontier Foundation,* 29 July 2011: <https://www.eff.org/deeplinks/2011/07/case-pseudonyms>.

[34] **I. R. Kerr, V. M. Steeves, C. Lucock (eds.).** *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press, 2009.

[35] **E. A. Whitley, I. Hosein.** *Global Challenges for Identity Policies*. London: Palgrave Macmillan, 2009.

[36] **A. Soltani, S. Canty, Q. Mayo, L. Thomas, C. J. Hoofnagle.** *Flash Cookies and Privacy*, 2009: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>.

[37] **M. Ayenson, D. J. Wambach, A. Soltani, N. Good, C. J. Hoofnagle.** *Flash Cookies and Privacy II: Now with HTML5 and eTag Respawning*, 2011: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390>.

[38] **G. J. D. Smith.** Exploring Relations between Watchers and Watched in Control(led) Systems: Strategies and Tactics. *Surveillance & Society*, 4(4): pp. 280-313, 2007.

[39] **E. Bumiller.** Air Force Drone Operators Report High Levels of Stress. *New York Times,* 18 December 2011: <http://www.nytimes.com/2011/12/19/world/asia/air-force-drone-operators-show-high-levels-of-stress.html>.

[40] **K. D. Haggerty.** Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance. *Critical Criminology*, 17(4): pp. 277-291, 2009.

[41] **S. A. Cole.** *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge: Harvard University Press, 2002.

[42] **J. Rosen.** Total Information Awareness. *New York Times Magazine,* 15 December 2002: http://www.nytimes.com/2002/12/15/magazine/15TOTA.html.

[43] **M. Williams.** The Total Information Awareness Project Lives On. *MIT Technology Review*, 26 April 2006: <http://www.technologyreview.com/news/405707/the-total-information-awareness-project-lives-on/>.

European Data Protection and the Haunting Presence of Privacy

Gloria González Fuster[1], Rocco Bellanova[2]

[1]Law, Science, Technology & Society (LSTS) Research Group, Vrije Universiteit Brussel (VUB) [2]Centre de Recherche en Science Politique, Facutés universitaires Saint-Louis; Law, Science, Technology & Society (LSTS) Research Group, Vrije Universiteit Brussel (VUB)

<Gloria.Gonzalez.Fuster@vub.ac.be>, <Rocco.Bellanova@vub.ac.be>

Abstract: *Since it first appeared in the 1960s, the legal notion of personal data protection has been living in the shade of the term privacy. Whereas in the United States (US) the regulation of the processing of information related to individuals was solidly framed under the privacy tag as early as the beginning of the 1970s, European legal orders were witnessing the emergence of concurring labels. Eventually, a genuinely European legal construct was to see the light of day: personal data protection, now recognised as a specific fundamental right of the European Union (EU), formally different from any right to privacy.At the core of the construction of the notion of personal data protection there is an attempt to steer clear of the private v. public distinction, on the grounds that the boundary between private and public, as well as any traditional conceptualisations of privacy in terms of intimate or private space, had been rendered inoperative by emerging technologies - concretely, by automated data processing. The notion of personal data protection proposed to structure reality from a different perspective, based on the distinction between personal and non-personal - terms that European data protection laws were soon to define for their own purposes. Almost 50 years after its genesis, European personal data protection still appears to be strikingly intertwined with the evolving notion of privacy. This contribution examines European data protection from the perspective of its relation(s) with privacy, sketching out both the distance between the two notions and their different entanglements. It devotes particular attention to the ongoing review of the EU data protection legal landscape, which seems (finally) to be announcing a formal emancipation of personal data protection from privacy but is at the same time built upon (hidden) references to it. Between claims and silences, privacy thus continues to play a role in the shaping of EU data protection. The importance of such a role is described with the help of Jacques Derrida's insights on the functioning of the word.*

Keywords: *Data Protection, European Union, Law, Personal Data, Privacy.*

Authors

Gloria González Fuster is a researcher at the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB), where she is completing a doctoral thesis on the right to personal data protection as a fundamental right of the European Union (EU), as well as contributing to the EU-funded Privacy and Security Mirrors (PRISMS) project. She has an academic background in law and communication sciences, and professional experience in different EU institutions.

Rocco Bellanova is assistant and researcher of the Centre de Recherche en Science Politique at the Facutés universitaires Saint-Louis (Brussels, Belgium) and researcher of the Law, Science, Technology and Society (LSTS) Research Group at the Vrije Universiteit Brussel (VUB). He holds a research master of political science and international relations of Sciences-Po Paris. His ongoing PhD research focuses on data protection applied to European security measures.

1. Introduction

In the last half-century, the death of privacy has been repeatedly proclaimed, and its erosion persistently announced. Its legal meaning appears to have been radically expanded, profoundly altered, but also dismissed, and forcefully questioned again and again. This contribution explores the ongoing reshaping of the European personal data protection legal landscape from the perspective of its relationship with such a fragile though resilient notion. More concretely, it examines the tensions between the conceptualising European personal data protection as an autonomous legal notion and envisaging it as part of a wider privacy notion.

In order to do so, this contribution first tracks down the origins of modern privacy in the United States (US), and follows its arrival in Europe. Second, it recalls the first steps of European personal data protection as an innovative legal notion, describing its original rationale. Against this background, it depicts some of the most striking elements of the relation(s) between privacy and personal data protection, giving particular attention to their practical entanglement in European Union (EU) law. Taking into account the ongoing major revision of the EU data protection legal landscape, it investigates the latest and contrasting developments of such an embroilment. Finally, it suggests that - without dismissing the influence of factors such as technological development - the common understanding of EU data protection law can be significantly enriched by giving due consideration to how words operate and to how law operates through words.

2. Emerging Technologies and the Redefinition(s) of Privacy

Emerging technologies have always played an outstanding role in the convoluted life of privacy. In the 1960s, the debate was particularly vivid in the United States (US). Diverse modern techniques and devices, ranging from the use of polygraphs for lie detection to the hidden tape recorder triggered public debate on the possible necessity to regulate them. Special inquiries were conducted to explore their potential impact on the rights and freedoms of the individual and in particular on individual privacy.

It was computers, however, that were soon singled out as encapsulating the major threat to society that required government action. At the beginning of the 1960s, computer makers started raising the alarm that the accumulation of information rendered possible by the new machines threatened to leave individual privacy at the mercy of the man in a position to press the button that made them 'remember'[1]. By the mid-1960s, the issue of 'computers and privacy' became a topic of official interest[2].

As it turned out that privacy was dangerously threatened by the advent of computers, the question became: how exactly does the computer endanger privacy? And what was privacy, in the first place? The 'right to privacy' had traditionally been conceptualised in the US as a "*right to be let alone*", following the impulse given by Samuel Warren and Louis Brandeis in 1890[3]. Their definition focused on the need to protect the individual against external interferences, such as, for instance, the publication in the press of pictures obtained through 'modern' photograph cameras. It was a conception of privacy that seemed to assume that privacy was the opposite of publicity[4], and that it was about keeping things 'private' in the sense of hidden, secret, or undisclosed. Could that conception cover the problems linked to the storage of computerised information?

To explain exactly how the computer threatened privacy, the notion was eventually broadened[5]. By the beginning of the 1970s, the word

> As it turned out that privacy was dangerously threatened by the advent of computers, the question became: how exactly does the computer endanger privacy?

privacy was thus re-defined as including a new dimension, reinvented as encompassing what was to be (sometimes) called 'informational privacy', or the right of individuals to determine for themselves when, how and to what extent information about them could be processed. Soon, however, this new meaning of the word started to prevail upon any other, at least in the context of discussions on emerging technologies. It was in this peculiar sense of privacy as informational privacy, and, *de facto*, with the exclusion of any other meaning, that the word was stamped on the major US act that since then ostensibly bears its name, the 1974 Privacy Act, marking the inclusion in US law of what has been qualified as a *"serious debasement"* of the term[6]. And it was in this particular new incarnation that the word privacy then crossed the Atlantic.

3. Europe and (no) Privacy

European countries had also been concerned since the 1960s with the impact of emerging technologies on human rights. Initially, the unease referred mainly to the spread of devices depicted as facilitating eavesdropping, such as hidden and directed microphones. As in the US, however, worries eventually concentrated on computers, and more concretely on the use of large computerised data systems by public authorities.

As the word 'privacy' landed in Europe, there was some general agreement on the opportunity of taking it into account, but also on the great difficulty in determining its possible relationship with European legal orders. European experts were very much aware of the debates in the US, and often alluded to the authors of privacy's re-invention[7]. Nevertheless, it was unclear how a general notion of privacy could – if at all – be translated into different languages. For instance, many Dutch-speaking scholars thought that, in Dutch, it would be better to incorporate it as such[8]. European countries had developed their own legal techniques to protect different specific facets of what could be envisaged as privacy. Typically, for instance, what was being offered was protection for private (in the sense of confidential) correspondence and for inviolability or sacred nature of the home, conceived as a private space, but the explicit recognition of a broad 'right to privacy' as a unitary right is a late phenomenon in Europe[9]. A common European legal notion under the name of 'privacy' was in any case nowhere to be found.

The word privacy is not mentioned in the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), signed on 4 November 1950, which constitutes the major European human rights reference. The Convention, equally authentic in English and French, formally protects in its Article 8 the right to respect for the private life (*vie privée)* of individuals, but does not refer to their privacy, in contrast to the international human rights instruments from which it is directly inspired[10]. As a matter of fact, the word privacy *almost* made it to the English version of Article 8 of the ECHR. Initial English draft versions of the text mentioned it, but the word was replaced by the expression private life only a few months before the signing of the Convention[11], allegedly to reinforce the impression of equivalence between the English and French versions.

The ultimate interpreter of the wording of the ECHR is the European Court of Human Rights (ECtHR), based in Strasbourg. Over the decades, the Court has construed the meaning of the expression private life of Article 8 of the ECHR very broadly, underlining that it cannot be reduced to an inner sphere of individual existence that would exclude social relationships and contacts with the outside world, but which, on the contrary, can definitely encompass them[12]. The Court has regularly taken great care to avoid using the word 'privacy' to refer to what is protected by Article 8 of the ECHR[13], and it has insisted on the need to read the expression 'right to respect for private life' as referring to the obligation not to interfere with the personal life of each individual[14], taking into account their personal autonomy[15], and therefore not framing it in terms of the defence of a 'private life' as opposed to a 'public life' or a 'private space' (as opposed to a 'public space')[16].

As such, the construction of private life by the ECtHR has no exact match in any national European legal order[17], although it has undoubtedly influenced all of them. Early comparative studies pointed out that what some called 'privacy' seemed to be protected under different names in some European countries[18].

Germany, for instance, granted somewhat similar protection through its Federal Constitutional Court's reading of a right to free development of personality protected in Article 2(1) of the German Basic Law. This Court eventually started to adopt a more privacy-sounding terminology, and developed in its case law what came to be known as the "*theory of the spheres*", incorporating different legal categories providing different degrees of protection based on distinctions related to degrees of 'the private'[19]. This case law contributed to the widespread use in German of the word *Privatsphäre* ('private sphere'), which has sometimes been used in EU law as the German equivalent to 'privacy'[20], even if intermittently *Privalebens* (a carbon copy of the ECHR's 'private life') replaces it[21].

France, which had paradoxically played a key role in contributing to early conceptions of the need to respect the 'private life' of individuals, in the context of the general need to respect individual freedom, explicitly incorporated in its legislation the need to protect the *'vie privée'* of individuals as late as 1970[22]. In the United Kingdom, the word 'privacy' was for many years regularly alluded to in important studies and unsuccessful legislative proposals with a variable scope, but for many decades failed to achieve any consolidated legal meaning.

4. Personal Data Protection as European Language

Instead of a consensus on how to incorporate or re-interpret privacy so as to better address the issue of the protection of individuals against the threats of computers, what Europe began to witness at the beginning of the 1970s was, in parallel with a continuous broadening of the concept of private life as construed by the ECtHR, the emergence of new, obliquely concurring notions.

> As the word 'privacy' landed in Europe, there was some general agreement on the opportunity of taking it into account, but also on the great difficulty in determining its possible relationship with European legal orders

> “As such, the construction of private life by the European Court of Human Rights (ECtHR) has no exact match in any national European legal order, although it has undoubtedly influenced all of them”

In 1970, the German Land of Hessen enacted its *Datenschutzgesetz*, or Data Protection Act. In 1973, Sweden adopted its *Data Lag*, or Data Act. These acts bear in their names the description of their objects: the German and Swedish words *Daten* and *data*, contrary to similar words coming from the Latin *datum* in other languages, do not refer to any kind information, but to information operated upon by machines[23]. Thus, these were acts aimed at regulating the automated processing of information. Soon after, France adopted similar legislation, though under a different tag, through which also resounded the need to regulate computerised data processing: '*informatique et libertés*'. Germany was itself not systematically loyal to the '*Datenschutz*' term, and not all the initial German acts related to the regulation of data processing were referred to by this name[24]. In addition, in 1983, the German Federal Constitutional Court granted constitutional-level protection to a right concerning the processing of personal data under a different *nomen iuris*, namely "*informationelle Selbsbestimmungsrecht*', or 'right to informational self-determination'[25].

In any case, it was the German expression *Datenschutz* that was eventually exported as a blueprint to all other European languages ('data protection') and managed to become the European way of approaching the legal issues related to the protection of individuals against automated data processing[26]. Furthermore, since 2000, the Charter of Fundamental Rights of the European Union formally recognises a fundamental right to the protection of personal data.

The emergence and consolidation of the notion of personal data protection in Europe not only marked a change of terminology, but also a crucial conceptual move away from any protection of anything 'private'. For data protection law, the determining factor to assess whether anything (for its particular purposes, any data) deserves to be protected or not, is whether or not it can be qualified as 'personal' - an adjective to be understood as 'relating to a particular person', i.e. to any identified or identifiable individual. If the data can be linked to somebody, then it is to be covered by data protection. The question of whether the data are 'private' or 'public' is, for the purposes of data protection law, irrelevant.

The logic behind this new approach relates to the difficulties of establishing genuine limits between 'private' and 'public' information[27], but also to the fact that even data that can be qualified as 'public', or that are obtained in so-called 'public' spaces can have an impact on the individual and, consequently, require some regulation.

The irrelevance of the private/public distinction for the purposes of data protection law echoes its lack of pertinence in construing the right to respect for private life as recognised by Article 8 of the ECHR by the ECtHR. The likeness between its broad interpretation of 'private life' and the scope of data protection has been recognised by the Strasbourg Court itself[28]. The Court has actually explicitly included under the scope of Article 8 of the ECHR elements of data protection, which in turn have confirmed and contributed to the stabilisation of the broad interpretation of 'private life'[29].

As an exception confirming the general rule, one can find in many data protection legal instruments special norms whose existence is based on the need to provide strengthened protection of some data. Indeed, in the beginning, there was some resistance to the idea that all 'personal data' deserve a degree of protection regardless of whether they could be described as 'private' or 'public'. As a sort of compromise between those favouring the protection of all 'personal data' and those opposing the idea, a new, 'mixed' category of data was invented: what was to be known as 'sensitive' data, or 'personal data' entitled for specially enhanced protection because of their peculiar nature, which links them to the intimate – e.g., data related to health, political choices or sexual life[30].

5. Embroiling Privacy and/or Data Protection

Despite the apparently sustained development of the protection of personal data as a fully-fledged autonomous legal notion in Europe, and despite the formal absence of the word privacy in the ECHR and in the Strasbourg case-law thereof, the term has remained at the forefront of many debates on law and technologies in Europe. Both external and internal factors help to explain this.

Privacy delineates a certain context of European data protection, which operates in a predominantly English-speaking world of global private companies, and among a profusion of data exchanges with the US. It has become the *lingua franca* word for the regulation of data processing. Privacy is the dominant term in the context of the Organisation for Economic Co-operation and Development (OECD)[31], and of the Asia-Pacific Economic Cooperation (APEC) forum[32] to refer to something that, like European data protection, is concerned with the processing of data related to individuals. As a result, the expressions data protection and privacy (understood as 'informational privacy') often co-occur in international discourse.

Privacy also features in European data protection law, acting on it from the inside. Even if there is no mention of privacy in Article 8 of the ECHR, data protection legal instruments adopted both at the level of the Council of Europe and by the EU have routinely asserted that there is. This practice can be traced back to 1968 when, in tune with the computers and privacy spirit of the 1960s, the Parliamentary Assembly of the Council of Europe adopted a Recommendation explicitly referring to the "*the right to privacy which is protected by Article 8*" of the ECHR[33]. This document led, eventually, to the adoption in 1973 and 1974 of two resolutions on data protection, and, in 1981, of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (generally known as 'Convention 108')[34], which explicitly recognised as its main purpose the need to secure the respect of the right to *privacy* of individuals (with regard to automatic processing of personal data relating to them)[35].

The major EU data protection instrument, Directive 95/46/EC[36], officially aimed at giving substance and amplifying Convention 108[37], and faithfully reflected its wording by identifying as its object the protection of fundamental rights and freedoms in general, but, in particular, the "*right to privacy*"[38]. As a result, even if Article 8 of the ECHR does not establish any 'right to privacy', it does so for the purposes of EU data protection law. Since the Strasbourg Court has affirmed that data protection is an integral part of the scope of Article 8 of the ECHR, it follows that data protection is part of (what itself refers to as) privacy.

Since 2000, the EU Charter of Fundamental Rights offers a different perspective on the issue. It consecrates personal data protection as a fundamental right in a specific article (Article 8), while reproducing the content of Article 8 of the ECHR, on the right to respect for private life, in its Article 7. It follows that, for the Charter, data protection is not part of (what EU data protection law designates as) privacy, but something running parallel to it, and therefore potentially autonomous. As the Charter acquired legally binding force in December 2009, this new and somehow contradictory approach acquired full legal validity.

From 2000 to 2009, however, the legal status of the Charter had been unsettled. The EU legislator, as if hesitating between adopting or ignoring its perspective, routinely incorporated in EU law various formulas which, by their ambiguity, nourished further hesitations. A famous example was the sentence "*privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data*", used in 2001 to describe possible grounds for refusal of access to documents. For a number of years, EU institutions intensely debated how that sentence should be read, with the European Data Protection Supervisor (EDPS) arguing that it meant that access to documents could be refused *only if* the individual's privacy (understood as something different to personal data protection rights) was affected, and the European Commission claiming that it meant that access had to be refused even if the disclosure simply affected somebody's data protection rights. In 2010 the EU Court of Justice adopted the latter view[39].

All in all, personal data protection appears to be sometimes understood as an *equivalent to privacy* (then interpreted as 'informational privacy' or control over personal information), sometimes as *an element of privacy* (then portrayed as a broad right, not limited to the protection of what is 'private' in the sense of opposed to 'public') and sometimes as *different from privacy* (then potentially contracted to a mere protection of the 'private' as opposed to the 'public'). Thus, personal data protection and privacy can relate to each other in various, seemingly conflicting ways, and the word privacy can conceal different meanings in relation to personal data protection, meaning which will be (temporarily) determined precisely by such relationships.

5. "A European Data Protection Framework for the 21st Century": Spectres of Privacy

European data protection is currently at an historic crossroads: EU institutions have embarked on the revision of the main instruments of the EU data protection legal framework. The legislative package presented to this end by the European Commission in January 2012, consisting primarily of a Regulation[40], a Directive[41] and a Communication[42] introducing both, is particularly illustrative of the complex relations between privacy and data protection. On the surface, the European Commission seems to be announcing the liberation of EU data protection from any reference to the right to privacy, incorporating the new instruments directly as the development of the EU right to the protection of personal data, now unambiguously portrayed as an autonomous fundamental right of the EU. At a deeper level, however, the force of privacy can be perceived as the original impetus behind various mechanisms suddenly re-named as data protection instruments, and, thus, also as the concealed path through which various future provisions might need to be read and interpreted.

> “ European data protection is currently at an historic crossroads: EU institutions have embarked on the revision of the main instruments of the EU data protection legal framework ”

The new Regulation proposed by the European Commission is to become the major future EU data protection legal instrument. It should replace Directive 95/46/EC, which, as highlighted, singled out as one of its objectives the insurance of the right to privacy. The text proposed by the European Commission for the upcoming Regulation obliterates such reference to privacy, to be replaced by a reference to the protection of personal data. Remarkably, despite this being a major proposed change in the wording of the very first Article of the new legal instrument, which is to determine the interpretation of all its other provisions, the European Commission has not acknowledged this as being a change requiring deeper discussion[43]. Nor does the European Commission ever point out that there are outstanding terminological differences between the Regulation and the Communication that is supposed to introduce it.

The proposed Regulation mentions privacy only in a limited number of cases: in relation to sensitive data[44] and data breaches[45], but little more. In contrast, the Communication uses it abundantly. As if privacy and data protection were synonymous, or, at least interchangeable words, the English version of the Communication is titled "*Safeguarding* Privacy *in a Connected World*", and subtitled "*A European* Data Protection *Framework for the 21st Century*". It explains that the European Commission, in order to reinforce EU data protection, is to encourage the use of use of *privacy*-enhancing technologies, *privacy*-friendly default settings and *privacy* certification schemes[46], as well as of the 'privacy by design' principle[47]. Should these occurrences of the word privacy be interpreted as meaning the same as data protection, or something different?

Read in conjunction with other language versions, all of them equally authentic for the purposes of EU law, the Communication reveals a fluctuating understanding of the word. In the German version, privacy has in some instances been translated as *Privatsphäre* (private sphere): 'privacy-enhancing technologies' are referred to as *Technologien zum Schutz der Privatsphäre*)[48]. In others, privacy has been replaced with *Datenschutz* (data protection): for instance, 'privacy-friendly default settings' are identified as *datenschutzgerechte Standardeinstellungen*. The Spanish and the Italian versions support the idea that the word privacy is used by the Communication in its own peculiar modern sense that none of these languages have ever attempted to fully translate – the Spanish version thus relies on systematically referring to *privacidad* (a loan translation from 'privacy'), and the Italian version on the direct borrowing of *privacy*.

If the interpretation of the word privacy in the Communication is uneasy, what is clear is that most of its potential occurrences in the Regulation have been replaced with allusions to data protection. The references to 'privacy by design' are especially demonstrative of the movements that have taken place between texts. Whereas the Commission announces in the Communication that it is introducing the principle of 'privacy by design', in the opening paragraphs presenting the Regulation it asserts that its provisions will set out obligations arising from the principles of 'data protection by design'[49], without providing any explanation on whether this might be something different, or new. There are no references to 'privacy by design' in the English version of the proposed text for the Regulation[50], but only to 'data protection by design' – except for one, actually, which seems to have survived as a residual proof that there were mentions of 'privacy by design' at some point of the drafting[51].

The (almost complete) replacing of 'privacy by design' by 'data protection by design' in the final text of the proposed Regulation[52] can be interpreted as suggesting that privacy and data protection *must* mean the same, because otherwise one could not function as a substitute of the other[53]. But it can also be perceived as the confirmation that they *do not* mean the same, or else there would be no reason for the substitution. In any case, what is certain is

> “This paradoxical situation is in our view best understood with the help of French philosopher Jacques Derrida and his insights into the dissemination of meaning through words”

that the notion of ‘data protection by design’ as presented in the proposed Regulation now harbours inside it the traces of the ‘privacy by design’ whose place it has taken. With it, the expression also carries the traces inhabiting privacy, which can include echoes of facets that ‘data protection’ as such was supposed to be *absolutely unconcerned with*, such as those related to any distinction between the private and the public. Thus, despite announcing a significant step towards the emancipation of EU personal data protection from privacy, the current review process of the EU data protection legal framework continues to fuel their entanglement.

6. Concluding Remarks

It is commonplace to assert that law changes (or can, or should change) in reaction to technological progress. While this is undoubtedly true, it is also true that language (the language that law is made of) has also a crucial role to play. In this contribution we have highlighted the role of the word privacy in the emergence and shaping of EU personal data protection. Debates on privacy and computers contributed significantly to its genesis, which nevertheless occurred outside any privacy framing – even if personal data protection was eventually to be deeply entangled with international privacy discourses. Privacy has played many contradictory roles in the progressive construction of EU protection of personal data: as a legal notion to be surpassed, as a concept contributing to its reshaping, as an intermittent *alter ego*, and, more recently, as a (sudden and uncommented) void to be filled.

We claim that European personal data protection should not, for the sake of accuracy, be generally described as privacy – not even as a sort of ‘informational privacy’. It is a legal notion which emerged historically as something different, and the specificity of which is being increasingly asserted in EU law. At the same time, we acknowledge that it can sometimes be accurately envisaged, referred, treated, interpreted as privacy, and that this word and the relationships to it are crucial for the existence of personal data protection. In a sense, it is the instability of the meaning of privacy that has kept and continues to keep personal data protection moving forward, despite the apparent disconnection of EU data protection law; like an inescapable spectre privacy still haunts it.

This paradoxical situation is in our view best understood with the help of French philosopher Jacques Derrida and his insights into the dissemination of meaning through words, and more particularly, on the construction of meaning in law as an incessant movement[54]. Taking as a starting point that legal text continuously displaces legal meaning[55], it follows that a word can encapsulate a multiplicity of linked readings, which can at a certain point be rendered visible (or invisible), supporting new readings of existing text. This way of meaning being forged is related to Derrida’s idea of *différence*, referring to the possibility for a word to conceal the key to many possible meanings, and by virtue of which the word is productive, in the sense that it can disseminate specific effects even through what it conceals[56]. In this sense, the complexities of the relation(s) between personal data protection and privacy in Europe, and their current seemingly paradoxical connections, are not just side-effects of mistranslations, or of incoherent legal interpretations, or of any factual error, but genuine phenomena inherent in the dissemination of meaning through words, and an illustration of the relevance of these phenomena to the understanding of law and of its evolution.

Notes

[1] **Vance Packard.** *The Naked Society*, Penguin Books, Harmondsworth, p. 49, 1971 (first published in 1964).

[2] Especially after in 1965 a report recommended that a centralised data system should store all information collected by the US government.

[3] **Samuel Warren, Louis Brandeis.** "The right to privacy", *Harvard Law Review,* 4(5), pp. 193–220, 1890.

[4] For an example of a defence of this conceptualisation, still popular in many fields: **Christena E. Nippert-Eng.** *Islands of Privacy*, The University of Chicago Press, Chicago, p. 4, 2010.

[5] See especially: **Alan F. Westin.** *Privacy and Freedom*, Atheneum, New York, 1970 (first published in 1967).

[6] **Roger Clarke.** "*What’s ‘Privacy’?*", paper presented at the Workshop at the Australian Law Reform Commission on 28 July 2006, available at <http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> [Last Accessed: February 2012].

[7] Notably, Alan F. Westin.

[8] As an example, in 1970 took place in Brussels the third conference edition of a series of Conferences devoted to the ECHR, titled in English *Privacy and Human Rights* and, in Dutch, *Privacy en Rechten van de Mens* (*Privacy en Rechten van de Mens: 3e Internationaal Colloquium over het Europees Verdrag tot Bescherming van de Rechten van de Mens [1970-Brussel]* (1974), Leuven, Acco).

[9] **Carlos Ruiz Miguel.** *La configuración constitucional del derecho a la intimidad*. Universidad Complutense de Madrid, Madrid, p. 76, 1992.

[10] See, notably, Article 12 of the Universal Declaration of Human Rights, which in 1948 asserted that "*no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation*".

[11] In the documents of the ‘travaux préparatoires’ of the ECHR the appearance of the expression ‘private life’ in the English draft can be dated to August 1950. Although it was common practice to underline in each new draft the changes proposed in relation to the previous draft, the sudden replacing of ‘privacy’ whit ‘private life’ was not identified as a change, and not underlined (Draft Convention adopted by the Sub-Committee on Human Rights (7th August 1950) (Registry of the Council of Europe (1967), *Travaux préparatoires de l’article 8 de la Convention européenne des Droits de l’homme -European Court of Human Rights: Preparatory work on Article 8 of the European Convention on Human Rights (Bilingual information document)*, CDH (67) 5, 12 May, Strasbourg, p. 17).

[12] Judgement of the ECtHR of 16 December 1992, Case of Niemietz v. Germany, Application no. 13710/88, § 29.

[13] The word tends to appear only exceptionally in a very peculiar context, namely each time that the ECtHR considers the possible relevance of the "*reasonable expectations of privacy*" doctrine (see, for instance, *Gillan and Quinton v. the United Kingdom, Application no. 4158/05),* Judgment of 12 January 2010, *§ 61*).

[14] Incidentally, this reverberates the original meaning of the Latin *‘privus’* as ‘singular’, ‘individual’ (**Ferdinand David Schoeman.** *Privacy and Social Freedom*, Cambridge University Press, Cambridge, p. 116), (1992, 2008).

[15] *Pretty v. the United Kingdom, no. 2346/02, § 61, ECHR 2002-III.*

[16] PG and JH v UK (Reports 2001-IX), Peck v UK (Reports 2003-I), and Perry v UK (Reports 2003-IX).

[17] **Kiteri García.** *Le droit civil européen: nouvelle matière, nouveau concept*. Larcier, Bruxelles, p. 185, 2008.

[18] In this sense, **Stig Strömholm.** *Right of privacy and rights of the personality: A comparative survey*. Boktryckeri AB Thule, Stockholm, 1967.

[19] **Robert Alexy.** *A Theory Of Constitutional Rights*, Oxford University Press, London, p. 236, (2002/2010). See in particular the Elfes judgment. Subsequent case law made it possible to identify three spheres of decreasing intensity of protection: the innermost sphere, a broader sphere of privacy, which embraces private life to the extent and a social sphere.

[20] See, for instance, the German version of the Directive 95/46/EC.

[21] See, for instance, the German version of the EU Charter ("*Artikel 7: Achtung des Privat- und*

Familienlebens").

[22] **Y. Détraigne, A.-M. Escoffier.** *Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et de l'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*. Sénat, p. 14, 2009.

[23] **Frits W. Hondius.** *Emerging data protection in Europe*, North-Holland Publishing Company, Amsterdam / Oxford, p. 84, 1975.

[24] For instance, on 24 January 1974 the Land of Rhineland-Palatinate adopted the *Gesetz gegen missbräuchlich Datennutzung.*

[25] In the *Volkszählungsurteil*, or Judgement for the Census, which also marked the overcoming of the "*theory of the spheres*" (**Mónica Arenas Ramiro.** *El derecho fundamental a la protección de datos personales en Europa*. Tirant Lo Blanch, Valencia, p. 392, 2006).

[26] Certainly not without hesitations and contradictions. Spain is perhaps the country that best illustrates the volatility of some terminological fashions, as the doctrine, the legislator, the judiciary have been subsequently succumbing to all possible loans from other European countries (leading for instance to the surfacing of expressions such as *'libertad informática', 'autodeterminación informativa',* or *'privacidad'*).

[27] **Pierre Kayser.** *La protection de la vie privée par le droit: Protection du secret de la vie privée*. Presses Universitaires d'Aix-Marseille, Marseille, p. 15, 1995 (3e édition).

[28] Judgement of the ECtHR of 16 February 2000, *Case of Amann v. Switzerland,* Application no. 27798/95, § 65.

[29] See notably: Judgement of the ECtHR of 4 May 2000, *Case of Rotaru v. Romania,* Application no. 28341/95.

[30] **Spiros Simitis.** "Les garanties générales quant à la qualité des données à caractère personnel faisant l'objet d'un traitement automatisé" in Centre d'informatique appliquée au droit de la Faculté de droit de l'Université Libre de Bruxelles (ed.), *Informatique et droit en Europe: Actes du Colloque organisé par la Faculté de Droit avec la participation de l'Association belge des Juristes d'Entreprises Belgische Vereniging van Bedrijfsjuristen les 14, 15 et 16 juin 1984*, Bruxelles, Éditions de l'Université de Bruxelles / Bruylant, p. 308, 1985.

[31] Involved in discussions on computers and policy since 1968, and responsible for the 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

[32] Which has its own Privacy Framework since 2005.

[33] **Council of Europe.** *Recommendation (68) 509 On Human Rights and Modern Scientific and Technological Developments*, adopted by the Assembly on 31st January 1968 (16th Sitting).

[34] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981.

[35] Article 1 of Convention 108.

[36] Directive 95/46/EC of the European Parliament and 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, *Official Journal of the European Communities*, L 281, 23.11.1995, pp. 31-50.

[37] Recital 11 of Directive 95/46/EC.

[38] Article 1(1) of Directive 95/46/EC.

[39] Judgment of the Court (Grand Chamber) of 29 June 2010, *European Commission v The Bavarian Lager Co. Ltd*., Case C-28/08 P, 2010 I-06051.

[40] **European Commission.** *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, Brussels 25.1.2012, Brussels.

[41] **European Commission.** *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, Brussels 25.1.2012, Brussels.

[42] **European Commission.** *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*, COM(2012) 9 final, Brussels, 25.1.2012.

[43] See, for the absence of justification for such change, the "*detailed explanations*" in COM(2012) 11 final, p. 7.

[44] Recital (41) of the proposed Regulation.

[45] Recital (67) and Article 32 of the proposed Regulation.

[46] COM(2012) 9 final, p. 6.

[47] COM(2012) 9 final, p. 7.

[48] Also in this sense, the title of the German version: "*Der Schutz der Privatsphäre in einer vernetzten Welt*".

[49] COM(2012) 11 final, p. 10.

[50] Recitals (61), (129) and (131) and Article 23 of the proposed Regulation.

[51] Article 30 of the proposed Regulation. This reference has no equivalent in any other language versions, except partially in those that appear to have been directly translated from the English version (such as the Portuguese).

[52] As well as parallel changes occurred for instance in relation to 'data protection (former privacy) impact assessments'.

[53] In this sense, the French version of the Communication already referred to '*protection des données dès la conception'* (or 'protection of data since the conception').

[54] **Jacques Derrida.** *Force de loi: Le "Fondement mystique de l'autorité*". Galilée, Paris, p. 51, 2005. ISBN: 2718604328.

[55] **Niklas Luhmann.** *Law as a Social System*. Oxford University Press, Oxford, p. 242, 2009 (see p. 236 for his embracing of Derrida's contribution).

[56] **Jacques Derrida.** *La Différance*. Conférence prononcée à la Société française de philosophie, le 27 janvier 1968, publiée simultanément dans le *Bulletin de la société française de philosophie* (juillet-septembre 1968) et dans *Théorie d'ensemble* (coll. Tel Quel), Ed. du Seuil, 1968. On the relevance for law of these ideas, see notably: **Pierre Legrand.** "On the Singularity of Law", *Harvard International Law Journal,* 47(2), pp.517-530, 2006.

Mathias Vermeulen
European University Institute, Florence (Italy)

<mathias.vermeulen@gmail.com>

Secrecy Trumps Location: A Short Paper on Establishing the Gravity of Privacy Interferences Posed by Detection Technologies

Abstract: *Since 9/11 the use of detection technologies has been increasingly seen as a crucial tool to counter terrorism. The use and deployment of these tools more often than not poses an interference with the right to privacy, including tools that are used in public places. In this contribution we will claim that the location where a privacy intrusive measure takes place is less of a determinant to establish the intrusiveness of a measure to the core of the right to privacy than the secrecy of such a measure.*

Keywords: *Detection Technologies, GPS, Human Rights Law, Privacy, Secrecy.*

Author

Mathias Vermeulen is a Research Fellow at the Law Faculty of the European University Institute (EUI) in Florence and a part-time researcher at the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB).

1. Introduction

According to the European Commission, the term 'detection technology' can refer to almost anything "*used to detect something in a security or safety context, with the focus on law enforcement, customs or security authority*"[1] .

Recently the EU counter-terrorism coordinator stressed the importance of detection technologies that enabled the investigation of IT services, the interception of telecommunications and the use of tracking devices (or other recording equipment) placed underneath or inside vehicles moving within the territory of several Member States. According to the EU counter-terrorism Coordinator the "terrorism phenomenon" is now "so specialized" that "*it can often be detected only with relatively sophisticated investigative techniques*"[2] .

The message that new technologies are needed to counter new threats of terrorism is not a new one. Thirty years ago the European Court of Human Rights (ECtHR) already stated the following: *Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction.*[3]

Little seems to have changed in the last 30 years: surveillance through the use of new technologies continues to be seen as a vital tool to prevent terrorist attacks.

At the same time concerns persist that these detection technologies threaten or violate the right to privacy. The European Court of Human Rights has developed a set of minimum safeguards regarding the use of specific detection technologies that are used in secret to intercept communications, but recently ruled in the Uzun case[4] that those safeguards are not applicable to secret surveillance with a GPS-device that tracked the movements of a suspect.

This contribution disagrees with that position, and argues that the principal factor determining the gravity of interference with the core of the right to privacy is not whether a technology detects the locations, movements or expressions of persons, but whether it does so secretly.

2. The Core of the Right to Privacy

Determining which elements of the right to privacy represent the 'core' of the right to privacy, or, in other words, are 'essential' is not a merely theoretical issue; it should affect the development, deployment and use of specific detection technologies. In X and Y vs. The Netherlands the Court for instance has indicated that the nature of the State's obligation to protect a right will depend on the particular aspect of private life that is at issue. In a case where "*essential aspects of private life are at stake*" the margin of appreciation is lower[5] . Addressing issues related to the protection of personal data will not suffice to determine the limits of the use of detection technologies. In this context the right is predominantly procedural: it informs the right to privacy and provides important parameters of control over some aspects of the private life of a person[6] .

The inviolable core of a right is a sub-category of a human right that is applied in an absolute fashion, so that within its scope of application, this core determines the outcome of the case, irrespective of any other legal arguments made. A right can carry more than one core, i.e. more specific norms to be categorized as a rule[7] .

In the case of privacy for instance, it could be argued that there exist at least two "core" areas. The first part relates to the 'essential' core of "pure privacy" and is similar to the *forum internum* dimension of freedom of religion, which refers to the internal and private realm of the individual against which no state interference is justified in any circumstances[8] . Similarly, the *forum internum* dimension of the right to privacy could consist of the right of an individual to own his/her own identity, or identities, including the right to change and not to disclose these identities.

A concrete aspect of this *forum internum* element of the right to privacy includes the freedom to express one's most intimate feelings or sexuality. In Germany the *Bundesverfassungsgericht* developed this element of the core of the right to privacy in a case regarding 'acoustic surveillance'. In this case the Court ruled that every act of surveillance has to be interrupted if there are indications that the surveillance will affect, inter alia, expressions of "innermost feelings or sexuality"[9] .

The second part of the core of the right to privacy focuses on its social value: its capacity to protect other human rights, including their core areas on the one hand and its enabling function for the enjoyment of other rights on the other. The right to privacy serves as a basis for other fundamental freedoms, such as freedom of expression, freedom of religion, freedom of association or freedom of movement. Without privacy these other freedoms would not be effectively developed and enjoyed[10] .

Interferences with the core of privacy lead to the infamous 'chilling effect', which is detrimental to democracy because it results in self-censorship in expressing deviant beliefs and inhibitions from doing 'unconventional' things. Interferences with this core of privacy threaten not only these activities, but also – in the words of Jeffrey Rosen "*gradually dampen the force of our aspirations to it*"[11] .

> “In the case of privacy for instance, it could be argued that there exist at least two "core" areas. The first part relates to the ‘essential’ core of "pure privacy" and is similar to the *forum internum* dimension of freedom of religion”

The right to privacy in this context functions primarily as a limit to the power of the state. Seen from this perspective it can be argued that the location where a privacy intrusive measure takes place is less of a determinant to establish the intrusiveness of a measure to the core of the right to privacy than the secrecy of such a measure.

Jeremy’s Bentham’s design for a Panopticon showed this already in 1791: being aware of the possibility of surveillance is just as inhibitory as actual surveillance[12]. Or, as Solove more recently highlights: "*In fact, there can be an even greater chilling effect when people are generally aware of the possibility of surveillance, but are never sure if they are being watched at any particular moment*"[13].

3. Challenges Posed by Secret Interferences with the Right to Privacy

The European Court of Human Rights has highlighted the threat of secret interferences with the right to private life in its case law under Article 8[14].

There are a number of reasons for this. The risk of arbitrariness in interferences with the right to privacy is greater when a power of the executive is exercised in secret[15]. Since secret measures take place without the knowledge of the individual who has been put under surveillance, seeking an effective remedy against this interference is rendered more difficult or even prevented. Often the individual concerned cannot take a direct part in any review proceedings of the interference either[16]. The Court has noted that this has an impact beyond the individual. In such a context, "*widespread suspicion and concern among the general public that secret surveillance powers are being abused*" would not be unjustified according to the Court[17]. In view of the risk of abuse intrinsic to "*any system of secret surveillance*", the Court has claimed that any such system "*must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated*"[18].

It seems to be undisputed that the only legitimate secret use of detection technologies can be in the context of the investigation or prevention of serious crime.

The European Court of Human Rights has stated for instance that secret telephone tapping is a "*very serious interference*" with a person’s rights and that "*only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorizing it*"[19].

It further indicated that the secret surveillance of citizens is only tolerable in so far as it is strictly necessary for safeguarding the democratic institutions, because a system of secret surveillance to protect national security entails the risk of "*undermining or even destroying democracy on the ground of defending it*"[20].

The European Court of Human Rights developed a strict set of minimum safeguards that should be set out in statute law in order to avoid abuses of power in cases of secret measures of surveillance: the nature of the offences which may give rise to the surveillance; a definition of the categories of people liable to be under surveillance; a limit on the duration of the surveillance; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the data should be deleted[21].

4. New Tools, New Challenges? GPS Trackers as ‘Public’ Detection Technologies

While the European Court of Human Rights has developed a set of minimum safeguards regarding the use of specific detection technologies that are used in secret to intercept communications, the Court recently said that these specific minimum safeguards which are to be set out in statute law are not applicable to secret surveillance with a GPS-device[22], because secret surveillance with such a device is considered to interfere less with a person’s private life than, for instance, telephone tapping[23].

The Court said that GPS surveillance: "*by its very nature*" is to be distinguished from "*other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person’s right to respect for private life, because they disclose more information on a person’s conduct, opinions or feelings*"[24].

The Court missed a chance here to fine-tune the right to privacy in the 21st Century. The Court did not take into account here the emerging importance of the concept of locational privacy, which may be defined as the ability of an individual to move in public spaces with the expectation that their location will not normally be systematically and secretly recorded for later use[25]. In the words of Beresford and Stajano, locational privacy is "*the ability to prevent other parties from learning one’s current or past location*"[26].

This concept is increasingly important as location data from GPS and mobile phones allow for the localization of an individual on a much wider scale, thereby enabling the correlation of individual behaviour to objects, places and other individuals[27].

Besides these two most important providers of location data (GPS and mobile phones), there are also a number of other techniques with which location information can be generated, including RFID (*Radio Frequency IDentification*) and biometric applications[28]. All this location data can paint a picture of the user’s communication behaviour, of his actions, whereabouts or movements, which can reveal details about personal profiles, relationships, and other aspects of personal life that would not ordinarily be observed by others.

Secret surveillance of location data should therefore not "by its very nature" be distinguished from visual surveillance. The secrecy of the measure makes it potentially equally threatening for the core of the right to privacy. Nowadays such surveillance for a prolonged period of time is able to disclose just as much information about a person’s conduct as an intercepted phone call, and the monitoring of such movements has an equally chilling effect on the enjoyment of other rights.

The argument above does not prevent one from arguing that the secret surveillance of personal expressions either by speech or text is a more serious interference with the core of the right to privacy. But it is unfortunate that the court chose not to apply the strict *Weber and Saravia* standards to the use of GPS trackers. The principal factor determining the gravity of interference with the core of the right to privacy is not whether a technology detects the locations, movements or expressions of persons, but whether it does so secretly. The distinction between detecting movements and

> It seems to be undisputed that the only legitimate secret use of detection technologies can be in the context of the investigation or prevention of serious crime

detecting expressions should come in only as a secondary step.

5. Conclusion

This short paper argues that detection technologies that are used in secret constitute the gravest interference with the core of the right to privacy; the distinction between detecting (public) movements and (private) expressions should only come in as a secondary step to determine the gravity of the interference with the right to privacy. Secret surveillance of location data should not by their "very nature" be distinguished from visual surveillance; they can reveal equally sensitive information and Courts should therefore attach as much importance to the procedural safeguards that are attached to the latter type of surveillance.

Notes

[1] COM (2006) 474, p.19.

[2] EU Counter-Terrorism Coordinator, Judicial dimension of the fight against terrorism – Recommendations for action, Doc 13318/1/10, 28 September 2010, at 3.

[3] European Commission on Human Rights. Klass and others v. Federal Republic of Germany, Application No. 5029/71, 1977, at para. 48.

[4] European Court of Human Rights, Fifth Section. Case of Uzun v. Germany (Application no. 35623/ 05), <http://ius.unibas.ch/fileadmin/user_upload/fe/file/EGMR_Uzun_v._Germany__2010_.pdf>.

[5] European Commission on Human Rights. X and Y v. The Netherlands, Judgment of 26 March 1985, para. 24-27.

[6] For a broader discussion see Paul De Hert, Serge Guthwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalism in action", in Serge Gutwirth, Yves Poullet, Paul De Hert, J. Nouwt, C. De Terwangne (eds.) "Reinventing data protection?" Springer Science, Dordrecht, 2009, pp. 3-44.

[7] **Martin Scheinin.** Terrorism and the pull of 'balancing' in the name of security, in Martin Scheinin (ed.), Law and Security - Facing the dilemmas. EUI Law Working Paper 2009/11, 2009, at 55.

[8] CCPR/C/21/Rev.1/Add.4, General Comment No. 22: the right to freedom of thought, conscience and religion, 30 July 1993, par.3.

[9] **G. Hornung, C. Schnabel.** Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention, Computer Law & Security Review 25, nr. 2 (2009): p. 117.

[10] **Martin Scheinin.** UN Doc. A/HRC/13/37, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 28 December 2009, para. 33 .

[11] **Jeffrey Rosen.** The Naked Crowd: Reclaiming Security and Freedom in an anxious age. London, Random House (2004), p.36.

[12] *"The Panopticon is a type of institutional building designed by English philosopher and social theorist Jeremy Bentham in the late 18th century. The concept of the design is to allow a watchman to observe (-opticon) all (pan-) inmates of an institution without them being able to tell whether or not they are being watched*". <http://en.wikipedia.org/wiki/Panopticon>.

[13] **Daniel Solove**. A taxonomy of privacy, University of Pennsylvania Law Review 154, nr. 3 (January 2006): p. 495.

[14] See most recently ECtHR, Weber and Saravia v. Germany, Application no. 54934/00 (Admissibility Decision) (2006)., par. 93; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application no. 62540/00 (2007), par. 75; Liberty and Others v. the United Kingdom, Application no. 58243/00, (2008) par.62; and Iordachi and Others v. Moldova, Application no. 25198/02, (2009), par.39.

[15] ECtHR, Bykov v. Russia (Application no. 4378/ 02),(2009) para. 78; Huvig v. France, Application no. 11105/84, (1990), at 29-32.

[16] See also European Commission on Human Rights, Klass and others v. Federal Republic of Germany, Application No. 5029/71. (1977), para. 52.

[17] ECtHR, Kennedy v. The United Kingdom (Application no. 26839/05) (2010), para.124.

[18] See ECtHR, Kopp v. Switzerland, Application n° 13/1997/797/1000,(1998) at 72; Weber and Saravia v. Germany, Application no. 54934/00 (Admissibility Decision) (2006), para. 93.

[19] ECtHR. Iordachi and others v. Moldova, Application no. 25198/02 (2009), para. 51.

[20] European Commission on Human Rights. Klass and others v. Federal Republic of Germany, Application No. 5029/71 (1977), para. 49.

[21] ECtHR. Weber and Saravia v. Germany, Application no. 54934/00 (Admissibility Decision) (2006), para. 95.

[22] ECtHR. Uzun v. Germany (Application no. 35623/ 05) (2010), para. 66.

[23] Idem. para. 72.

[24] Idem, para. 52.

[25] **Andrew J. Blumberg, Peter Eckersley.** "On Locational Privacy, and How to Avoid Losing it Forever" (Electronic Frontier Foundation, August 2009), p. 2.

[26] **A.R.Beresford, F. Stajano.** "Location Privacy in Pervasive Computing". IEEE Pervasive Computing, 2(1), pp. 46-55.

[27] **Ronald Leenes.** Mind my step?, TILT Law & Technology Working Paper Series, nr. 011 (2009): p. 6.

[28] Nouwt, ibid. note 22, at 381.

Darren Palmer[1], Ian Warren[2]

[1]Chair Australian Surveillance Studies Group, Criminology, School of Humanities and Social Sciences, Deakin University, Geelong (Australia); [2]Senior Lecturer in Criminology, Australian Surveillance Studies Group, School of Humanities and Social Sciences, Deakin University, Geelong (Australia)

<{darren.palmer,ian.warren}@deakin.edu.au>

Surveillance Technology and Territorial Controls: Governance and the 'Lite Touch' of Privacy

Abstract: *The considerable growth of surveillance technologies, dataveillance and digital information processing has occurred across many domains, including the night-time economy. We explore a particular technology (ID scanners) and the connections between this form of surveillance and associated database construction with the broader use of new forms of territorial governance. In turn, we argue that privacy, at least in the context of Australia, has limited influence on the use of new and untested surveillance technologies in contemporary law enforcement. In part, this is due to the construction of current Australian privacy laws and oversight principles. We argue this in itself does not solely account for the limitations of privacy regimes, as recent Canadian research demonstrates how privacy regulation generates limited control over the expansion of new crime prevention technologies. However, a more telling problem involves the enactment of new laws allowing police and venue operators to exclude the undesirable from venues, streets and entertainment zones. These developments reflect the broader shift to governing through sub-sovereign territorial controls that seek to leverage many current and emerging surveillance technologies and their normalisation in preventing crime without being encumbered by the niceties of privacy law.*

Keywords: *Alcohol, Antisocial Behaviour, Crime Prevention, Economy, ID Scanners, Night-time, Privacy.*

Authors

Darren Palmer is an Associate Professor in criminology at Deakin University, Geelong, Australia. He is a co-editor of *Crime and Justice: A Guide to Criminology* (2012) and *The Global Environment of Policing* (2012); co-author (with Ian Warren) of *Global Justice: Theories, Practices and Impediments* (2013), a forthcoming chapter (with Ian Warren) 'Re-territorialising Urban Governance in Australia' in R Lippert and K Walby eds. *Policing Cities: Urban Securitization and Regulation in a 21st Century World*, and currently preparing a manuscript on ID scanning in the Night Time Economy (with Ian Warren and Peter Miller).

Ian Warren is a Senior Lecturer in criminology at Deakin University, Geelong, Australia. He has written extensively on various important social issues relating to crime, drug law enforcement, surveillance and regulatory control. Most recently, he has been involved in a major research examining the use of ID scanning technologies to prevent violence and anti-social behaviour in Australian licensed venues.

1. Introduction

A quick glance at most privacy legislation indicates personal information provided for a business or commercial purpose must be provided to law enforcement authorities upon request. In the case of Australia, this information must be provided to these authorities for 'the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law' ([1], Schedule 1). This broad and ill-defined exemption indicates that the protection of personal information is secondary to the demands of criminal law enforcement, evidence gathering, the prevention of crime and the goal of community protection [2][3][4].

Privacy law potentially mediates the schism between surveillance, reactive criminal detection and crime prevention. However, the example of Australia indicates the reality of privacy law as a substantive mediating force against the growing tendency to use surveillance technologies in contemporary criminal justice is much less clear.

For two decades privacy scholars have outlined the social benefits of taking privacy more seriously [5][6]. All Australian state and federal jurisdictions have robust legal structures enabling Privacy Commissioners to work with private industry and oversee the development of codes of practice relating to the collection, storage and accurate maintenance of personal information for business purposes. Human rights instruments also contain specific references to privacy that are enforceable against state Parliaments, courts, tribunals and relevant statutory authorities. For example, as long as there are no competing national laws that enable government intrusions into the private domain, Victorian law confers two main rights to privacy on all individuals that are enforceable against public authorities operating within that state:

a) [The right] not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and

b) [The right] not to have his or her reputation unlawfully attacked ([7], section 13).

These principles focus mainly on intrusions into the private home, with the emphasis on personal reputation being more akin to the power of defamation law to prevent unnecessary snooping and gossip about personal activity. However, any untoward intrusions that occur beyond the private or personal realm remain beyond these legal protections. Nevertheless, the ability to access goods and services, or the adoption of new technological strategies in public and semi-public spaces remains a growing facet of contemporary life [8], with the nexus between safety, security and information privacy extending well beyond those rights protected by most current Australian laws.

Australian state and federal privacy legislation allows concerned citizens to question the measures adopted by private businesses to solicit or maintain personal information for the provision of goods or services [1][9]. Regardless of how frequently these measures are activated by concerned citizens, any personal legal rights to privacy or any codes of practice developed between private industry and designated Privacy Commissioners do little to erode the function creep of new technologies in the delivery of commercial or governmental services.

Growing demands for providing quicker and more efficient ways of delivering services to ordinary citizens [10][11] also extend to the law enforcement field, where police agencies increasingly rely on new technologies to enhance their investigative, crime prevention or mass surveillance capacities. For example, road traffic control is one area of law enforcement that has become so dependent on new surveillance technologies that the administration of fines and other punishments for problematic driving is almost fully automated. This form of simulated justice [12] comes at considerable cost, particularly when police managers or operational personnel fail to adapt conventional modes of enforcement to ensure new technologies are deployed according to accepted due process requirements [13].

> “The example of Australia indicates the reality of privacy law as a substantive mediating force against the growing tendency to use surveillance technologies in contemporary criminal justice is much less clear”

A recent Ombudsman's report examining the implementation of new data management systems in several Victorian government departments is particularly critical of the lack of coordinated leadership behind the deployment of many technological initiatives in contemporary public administration [14].

A crucial example involves the protracted efforts to upgrade the Victoria Police crime database. The report identified considerable financial waste stemmed from the absence of clear managerial oversight of the implementation of this important upgrade. More importantly, this lack of a strategic long-term vision meant that any new data management and dissemination strategies were adopted without adequate consideration of the future objectives of the organisation. The report concluded that the Victoria Police was clearly unwilling to adapt its 'business processes to fit the new system', because it was preoccupied with making 'the system fit Victoria Police's [existing] processes' ([14], p. 66). The end result was the ultimate abandonment of the database upgrade after five years of preliminary work and the expenditure of tens of millions of dollars. The cause of this wastage was simple: Victoria Police had not 'defined and set a clear vision for modern policing out to 2030', established clear business requirements, adequately planned for organisational transformation from a paper-based organisation to an electronic organisation or established clear ownership and accountability for organisational transformation ([14], p. 66).

The sense of mistrust associated with these large-scale publicly funded databases filters into the routine uses of new technologies to supplement conventional operational policing activities. Here, extensive reforms to the criminal law introduce lower legal thresholds to combat minor forms of crime or antisocial behaviour [15], which fuel more intrusive forms of mass surveillance in both public and semi-public spaces. These developments can have several negative social impacts [16][17]. While much has been written about the contemporary 'reflex application of the criminal law … to deal with complex social problems' ([18], p. ix), the use of technology by police or private agencies, such as open space CCTV systems or mobile phone tracking devices in large privately owned shopping malls, increases the scale of dataveillance in contemporary life. This in turn helps to normalise the use of questionable information technology and data mining practices for fairly routine low-level law enforcement activities.

The power of existing privacy laws to contain both the nature of such information gathering and the desirable uses of personal data is limited in two ways.

First, there is little scope for privacy law to allow citizens to collectively challenge the growing function creep of new surveillance technologies employed by police, other government departments or private businesses. As with many other areas of law, the right to correct an actual or suspected privacy breach can only be determined after an aggrieved person has detected a suspected violation by providing sufficient evidence of harm to convince a court or other official body that legal intervention is required. This 'back-end' process is partially tempered by Australian Privacy and Information Commission structures, which enable the development and implementation of codes of practice to prevent breaches of agreed standards by private businesses or local governments. These processes are yet to be researched in depth in Australia. However, emerging research into similar oversight methods in Canada indicates that extremely diverse standards of information management are developed for the administration of open space CCTV networks, which undermines consistency in the application of privacy law. Moreover, Commissioners routinely prioritise public safety over individual or collective privacy interests when developing methods of overseeing the operation of these systems and related data access, storage and maintenance protocols [19].

Second, these processes are fuelled by the express exemption under Australian privacy law regarding crime. This crucial term has yet to be scrutinised in detail by Australian courts. The complex relationship between crime prevention [20], technology and privacy adds weight to Hier and Walby's [19] concerns regarding the value of current privacy laws in protecting the community from the expanded uses of intrusive surveillance technologies or the data they generate. As Solove [21] indicates, the emotive nature of crime and security debates establishes an uneven playing field where the privacy interests of few are considered to unnecessarily compromise the safety of the majority. Solove's concern is that the failure to equate privacy with greater security means that in any debate between these two important social concerns, security and community protection will always win. This means privacy rights run the risk of dissolving as more surveillance technologies permeate the contemporary crime prevention landscape, even if, as the Victorian example indicates, both the high- and low-end uses of these forms of dataveillance are not necessarily matched by shifts in the prevailing enforcement philosophies that inform their deployment.

One area where these debates are prominent is within the management of the contemporary night-time economy. In recent decades law enforcement agencies, often working alongside community groups and venue proprietors, have faced growing pressure to strategically identify and prevent the risks of collective violence, antisocial behaviour and disorder in and around licensed venues [22]. This push has generated extensive reforms to enable increased surveillance of those participating in the night-time economy, along with a greater range of fines and other punishments for more trivial forms of unruly behaviour. The following discussion builds on our extensive research into the use of computerized ID scanning in the Australian night-time economy by challenging the common assumption that new surveillance technologies automatically make the night-time economy safer or easier to manage. More importantly, information privacy law appears largely incapable of preventing the normalization of this form of surveillance. This trend is especially problematic when viewed in conjunction with the introduction of zonal banning laws aimed at removing disorderly people from individual venues, nightclub precincts or designated zones incorporating the central business districts (CBDs) of Australia's urban and regional cities.

2. ID Scanning, Function Creep and Privacy in Australia

Mandatory patron ID scanning has become an increasingly popular method of attempting to minimise the prospect that disorderly or violent people will enter nightclubs or entire entertainment precincts in many Australian cities. This technology enables proprietors to take a digital image of a patron's identification document and a photograph or biometric identifier, such as a fingerprint, prior to allowing entry into a venue licensed to sell alcohol. The person's identity can then be instantly matched with manual records entered into the database that alert door staff about patrons who have been banned from

> "The person's identity can then be instantly matched with manual records entered into the database that alert door staff about patrons who have been banned from the venue"

the venue. As a recent Victorian report on *Surveillance in Public Places* indicates, one major casino in Melbourne has deployed: "*... [i]dentification scanners [to] record the image and written details on an individual's driving license or other identity card, including their name and address. Facial recognition software scans patrons' faces as they enter the nightclub and matches those images against a database of photos. In this way the software can be used to identify patrons who have been previously banned from a venue. The software can be shared among venues*" ([23], p. 40).

Unlike some United States jurisdictions [27] where ID scanners have been specifically endorsed in state liquor licensing laws, many systems in Australia have been adopted at a piecemeal level at the discretion of individual venue operators. However, at least two regions in Australia have seen a more formal approach to the use of ID scanners alongside several additional measures aimed at combating alcohol-related harm.

In March 2010 the Queensland Parliament Law, Justice and Safety Committee released an extensive report outlining 'best practice' in the management of alcohol supply within that state. The report emerged from concerns that Australia's historical 'knock 'em down' attitude towards alcohol consumption and mateship, had given way to: "*... a growing culture of [binge] drinking to harmful levels, without any pride or self-respect. Vomiting, falling over, and creating a nuisance in public are not seen as shameful but to some are badges of honour. A lack of self-respect and respect for others seems entrenched*" ([24b, p. i).

A series of public hearings, venue site visits by Committee members and written submissions by various 'stakeholders', including liquor industry representatives, legal services, youth advocacy groups and education providers, generated an extensive report examining the causes of alcohol-related violence and offered several proposals to improve venue amenity, transport, responsible service of alcohol guidelines and the use of surveillance technologies to manage behaviour in the night-time economy. A total of sixty-eight recommendations were proposed, ranging from formal amendments to criminal and summary offence laws, to the more stringent implementation of national public health programs targeting young people in schools and other community settings.

The final report recognised that ID scanning had been adopted by a number of venues throughout Queensland and in several cases was successfully '*used in conjunction with CCTV images to identify offenders*' ([24b], p. 24). In some 'high risk areas' where more than one premises had deployed this technology, system networking allowed a quick and easy method of determining that a patron banned from one premises should not be allowed entry into another. Various organisations, including the Queensland Police Union of Employees and the Liquor Hospitality and Miscellaneous Union, supported this technology due to its potential to deter troublemakers and enable police to efficiently identify those engaging in violent or antisocial behavior.

The following submission from the Chief Executive of the Queensland Hotels' Association aptly captures the positive view of this technology: "*We have introduced ID scanning where the appropriate form of ID is scanned at the point of entry, and that acts as a clear deterrent to patrons who might otherwise be intending to get up to no good. People know that, if their identity is held in a safe computer and if they create harm or create violence or break the law, those people who are authorised to access the hard drive, being the Police Service, will be able to track them down*" [24b, p. 25).

However, a lengthy submission from the Queensland Information Commissioner raised several concerns over the desirability of extending the use of ID scanners pending the development of agreed information management standards, or more detailed discussion of their legal implications under current Queensland and national privacy legislation. Two main concerns informed this submission. The first involved reservations about the causal link between alcohol and violence in the public imagination. This had the potential to place undue reliance on ID scanning as a quick and effective 'technological fix' [25] to the problem of drinking culture, at the expense of other less intrusive harm minimization strategies. The second relates to the use of dataveillance to achieve substantive improvements in social order. Not only is the deterrent effect of ID scanning difficult to establish, but real concerns also surround the monitoring of *all*venue patrons through such technology. This means that 'the collection of personal information by licensed premises' is more likely to involve questionable forms of dataveillance, with ID scanners becoming '*the all seeing eye for law enforcement by police*' ([24b], p. 25).

While Queensland has not been plagued by the same difficulties surrounding the adoption of new law enforcement technologies that were identified by the Victorian Ombudsman [14], the relatively unquestioned acceptance of ID scanning technologies, either with or without an appropriate trial or adequate consideration of their privacy implications, presents numerous problems. Importantly, many other situational and supply-based policy interventions can have a meaningful impact in altering negative drinking cultures. Nevertheless, despite these concerns the final report recommended licensees trading after midnight should be encouraged to install ID scanning systems with 'due regard to privacy issues and matters of natural justice' ([24b], p. 27).

Neither the report nor the government's formal response clarifies the specific implications of the terms 'due regard' or 'natural justice'. It was suggested venues should receive discounted licensing fees for installing ID scanners, but this proposal was ultimately abandoned with the Queensland government introducing a 'new more secure, more durable and more reliable driver license card' in 2010 ([26], p. 5). More problematically, this example illustrates how Australian governments appear willing to override key issues relating to information privacy given the seemingly more pressing demands of combating alcohol-related disorder through expanded and untested surveillance measures. Interestingly, the Committee's interim report recognised both 'the safety of patrons and the protection of their identity documents are paramount' and strongly cautioned against the widespread use of networked ID scanning until these issues were adequately addressed ([24a], p. 8).

The mandatory adoption of ID scanning in the 'high risk' venues trading after 1.00 am in the Victorian city of Geelong followed a slightly different trajectory. In response to several widely publicised violent crimes in the city's nightclub precinct during late 2006, police, venue proprietors, the local council and concerned citizens used a voluntary Liquor Accord to reform the night-time economy within the 2.5 square kilometre CBD. This region contains up to ten licensed hotels that are popular amongst the local population, large numbers of university students and holidaymakers venturing to Victoria's coastal resorts during the summer months [28]. Key

> “ Neither the report nor the government's formal response clarifies the specific implications of the terms 'due regard' or 'natural justice' ”

stakeholders involved in the Geelong Liquor Accord agreed to pilot ID scanners at ten venues between May and November 2007. However, neither the initial pilot, nor the formalisation of this technology as a mandatory condition of entry into all high-risk venues under the revised Accord that was released in November 2007 met with any substantial public debate [28].

As with the earlier introduction of CCTV, there was no attempt to develop legal regulation and deliberation processes for determining authorization and appropriateness of the use of ID scanners (for a contrasting example see [29] on the legal regulation of CCTV in Spain).

The most significant event occurred after November 2007 and involved reforms to Victoria's liquor licensing laws that introduced an expanded banning order procedure originally applying to ten designated areas across the state including the Geelong CBD. Section 148B of Victorian *Liquor Control Reform Act* [40] now enables police to implement a zonal ban preventing a person from entering a designated area for behaviour considered to 'give rise to a risk of alcohol-related violence or disorder'. The bans apply to relatively minor public drunkenness or obscene language offences, or more serious assaults, sexual assaults and unlawful weapons offences occurring within the zone ([40], Schedule 2).

All of these behaviours were already prohibited under existing state criminal laws. When coupled with a short-term ban, a person is subject to a $500 fine and must immediately leave the designated area for up to 72 hours unless they live or work within the zone. Failure to comply with the ban carries additional fines and the prospect of an extended banning order, which can also be imposed as a punishment for any serious offences committed 'wholly or partly in a designated area' attracting a maximum imprisonment term of less than 12 months. In these cases, police, the Office of Public Prosecutions or a court must be satisfied the extended order '*may be an effective and reasonable means of preventing the commission … of further specified offences in the designated area*' ([40], s. 148I(1)(c)).

Available data indicates that in the first six-months of operation, the Victoria Police used these banning powers sparingly. From December 2007 to 30 June 2008, 129 bans were issued to 128 'unique persons', with one person being banned on two occasions. All bans were implemented in Melbourne CBD and surrounding declared areas, where there are far greater concentrations of nightclubs than the less populated Geelong zone. Only six per cent of people receiving bans in this initial period were women, while 66 per cent were in the 20-29 year age category. A further 22 per cent were under 20 years of age, while 9 per cent were between 30 and 39 years of age ([30], p. 9).

Periodic government media releases on official websites or in Victorian newspapers reveal that between December 2007 and January 2010, police issued 2,492 short-term banning notices. Around 95 per cent of bans were directed at men, with 2,144 orders issued in the Melbourne CBD ([30], p. 9) [31].

After a change of government in December 2010, this banning regime was expanded to cover several additional public order offences, while increased fines now accompany on-the-spot bans and subsequent breaches of short- or longer-term banning orders. In addition, the banning powers now apply to three new designated areas [32] and further provisions enable police and all venue managers and their security staff in Victoria to impose a graded series of bans ranging from one to six months for various alcohol-related offences occurring in or near individual venues. These 'barring orders' attract fines of up to $2000 if a banned person is detected within 20 meters of the venue where the order applies ([40], s. 106).

The methods for enforcing either short-terms bans issued by police, venue operators and security personnel, and the extended bans imposed by a magistrate's court, are not stated within the relevant legislation. While available data indicates only sixteen bans have been imposed in Geelong between December 2007 and December 2009 ([30], p. 9), the relatively systematic introduction of ID scanners amongst the high-risk venues in this city provides an enforcement template for other designated areas to follow. Enhanced information networking between venues also now makes the task of enforcing bans and increased fines for these low-level liquor violations in the Geelong designated area potentially much easier.

However, questions regarding data security and information privacy remain squarely outside the official discourses that support these new surveillance measures. Of particular concern is the lack of agreed protocols that enable patrons to enter a venue in the Geelong CBD without having their identity scanned. The common practice is to insist that ID scanning is a mandatory requirement before entry is permitted. If patrons decline this requirement, they are routinely told '*… its for security … (w)e just say it's the law*' ([33], p. 22).

The philosophy underpinning this approach is simple. Venue managers believe ID scanners are a valuable method of promoting venue safety by allowing security personnel to 'quickly identify [troublesome patrons] and ban them' ([33], p. 22). Any countervailing concerns over information privacy, data security or police access to scanned information are secondary to the overriding belief that ID scanners can efficiently identify patrons banned from venues deploying this technology, or that they are a valuable deterrent against troublesome or underage patrons attempting to enter any licensed premises within the Geelong CBD.

3. Conclusion

Like many other forms of dataveillance, ID scanners contribute to new forms of 'particularized' citizenship that can compromise universal or rights-based access to government and private services ([10], p. 731). While such measures can enhance community safety, they can also exacerbate social 'segmentation' when supplemented by 'multiple hybrid, civil, contractual, and administrative' legal requirements aimed at regulating a growing number of 'irregular citizens' or 'antisocial youth' ([17], p. 389; 394-397).

There are numerous unknown questions surrounding how police manage and use the data obtained from participating nightclubs in the Geelong CBD to help enforce Victoria's banning regime. Data security, the manual entry of a banned designation and protocols over information sharing, all of which are subject to many legally enshrined privacy controls, remain to be clarified given the overriding importance of promoting safer night-time economies through more intrusive forms of computerised surveillance.

The Queensland report also advocated replicating the Victorian legislative model by introducing the '*power for police to ban trouble patrons from entertainment precincts for 24 hours' and allowing 'courts to issue a banning order where there is persistent alcohol-related*

> “While individuals might be able to bring a legal challenge under the Victorian *Charter of Human Rights and Responsibilities Act*, these provisions relate to personal breaches rather than the processes that lead to the adoption of new surveillance technologies”

offences committed by a person, or where a person commits a serious offence in or around licensed venues' ([24b], p. 23).

This effectively means individuals are increasingly subject to surveillance through their ‘digital footprints’ and personal ‘trust profile(s)’ ([10], p. 730), which police and venue operators monopolise through ‘exclusive [digital] knowledge’ sharing about troublesome persons and their activities ([34], p. 59). Both the Queensland and Geelong examples indicate local and state governments are more than willing to concede that privacy protection is an outlying concern that can be dealt with after these processes are introduced.

Moreover, the firms that manage the installation and maintenance of this technology are able to ‘*share a banned list of troublemakers – whether that listing is local, statewide or national*’ [35]. This raises additional concerns that such forms of computerised surveillance know few geographic boundaries.

The urgency of promoting increased safety in the night-time economy means the impact of problematic ‘back end’ assemblages involving scanned personal data is only challengeable through administrative, rather than criminal law. Privacy and natural justice processes involve establishing whether the use of these technologies conforms to agreed minimum standards, rather than a detailed assessment of the impact of this ‘surveillance creep’ ([36], p. 181) on individual or collective citizen rights.

While individuals might be able to bring a legal challenge under the Victorian *Charter of Human Rights and Responsibilities Act*, these provisions relate to personal breaches rather than the processes that lead to the adoption of new surveillance technologies. Privacy law can enable citizens to review and correct personal information stored in any venue database if there has been an error in recording a ban applying to a particular venue or designated zone. Broader constitutional arguments regarding freedom of movement have yet to be raised under current Victorian human rights law, but remain an obvious site for further investigation given the potential social impacts of these zonal prohibitions [37].

Most problematically, these forms of surveillance are inadvertently validated under conflicting legal regimes that ‘erode privacy rights, create new forms of inequality, and lack mechanisms of accountability’ ([38], p. 6). This is particularly concerning given that any determination of whether a person should be banned from a particular venue or designated zone involves highly discretionary judgments by police, venue operators and private security personnel.

Through an emphasis on increased security, crime prevention and greater community protection, these novel and untested forms of computerised surveillance do compile more detailed and potentially accurate information on people and their activities both within and across Australian state borders. However, when combined with expanded legal powers, such as the Victorian banning provisions, these new forms of simulated surveillance [39] and justice [12] question the value of information privacy law in establishing appropriate information collection and data management strategies before these technologies become normal facets of social life.

The political tendency to introduce and endorse these technologies without adequate public debate is arguably fuelled by the current legal exemption of crime under contemporary Australian privacy law. By conferring few rights to enable citizens to directly challenge the adoption of these security technologies, privacy law inadvertently vests enormous trust in police and other commercial service providers to appropriately manage their deployment. As the recent inquiry in Victoria illustrates, there is serious doubt over whether such trust is deserved.

References

[1] *Information Privacy Act*, Victoria, 2000.

[2] **W. Schinkel.** Prepression: The actuarial archive and new technologies of security. *Theoretical Criminology*, 15(4): 365-380, 2011.

[3] **C. Osmond.** Anti-social Behavour and its Surveillant Inter-assemblage. *Surveillance and Society*, 7(3-4): 325-343, 2010.

[4] **S. Thompson, G. Genosko.** *Punched drunk: Alcohol, surveillance and the LCBO, 1927-1975*, Blackpoint, Nova Scotia: Fernwood Publishing, 2009.

[5] **D. Lindsay.** An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law. *Melbourne University Law Review*, 29(1): 179-217, 2005.

[6] **G. Greenleaf, N. Waters, L.A. Bygrave.** Implementing privacy principles: After 20 years its time to enforce the Privacy Act. *University of New South Wales Law Research Series*. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=987763> [Accessed on 2 November 2010].

[7] *Charter of Human Rights and Responsibilities Act*, Victoria, 2006.

[8] **J.B. Rule.** *Privacy in Peril: How We are Sacrificing a Fundamental Right in Exchange for Security and Convenience*. New York, NY: Oxford University Press, 2007.

[9] *Privacy Act*, Commonwealth, 1988.

[10] **A. Lips, B. Miriam J.A. Taylor, J. Organ.** Identity management, administrative sorting and citizenship in new modes of government. *Information, Communication & Society*, 12(5): 715-734, 2009.

[11] **G. Greenleaf.** Access all areas: Function creep guaranteed in Australia’s ID card bill (no. 1). *Computer Law & Security Report*, 23(4): 332-341, 2007.

[12] **P. O’Malley.** Simulated Justice: Risk, Money and Telemetric Policing. *British Journal of Criminology*, 50(5): 795-807, 2010.

[13] **P.K. Manning.** A View of Surveillance. En *Technocrime: Technology, Crime and Social Control*, S. Leman-Langlois (ed.). Cullompton UK: Willan Publishing, 2008.

[14] **Victorian Ombudsman.** *Own Motion Investigation into ICT-Enabled Projects*. Melbourne, Vic: Victorian Government Printer, 2011. http://www.ombudsman.vic.gov.au/resources/documents/Investigation_into_ICT_enabled_projects_Nov_2011.pdf [Accessed on 9 March 2012].

[15] **R. Matthews.** Beyond ‘so what?’ criminology: Rediscovering realism. *Theoretical Criminology,* 13(3): 341-362, 2009.

[16] **A. von Hirsch, A.P. Simister (eds).** *Incivilities: Regulating offensive behavior*. Oxford, UK: Hart Publishing, 2006.

[17] **L. Zedner.** Security, the state, and the citizen: The changing architecture of crime control. *New Criminal Law Journal*, 13(2): 379-403, 2010.

[18] **N. Des Rossiers, S. Bittle.** Introduction. En *What is Crime? Defining Criminal Conduct in Contemporary Society*, Law Commission of Canada (ed.), Vancouver: UBC Press, 2004.

[19] **S.P. Hier, K. Walby.** Privacy Pragmatism and Streetscape Video Surveillance in Canada. *International Sociology*, 26(6): 844-861, 2011.

[20] **A. Sutton, A. Cherney, R. White.** *Crime Prevention: Principles, Perspectives and Practice*s. Melbourne, Vic: Oxford University Press, 2008.

[21] **D.J. Solove.** *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, CT: Yale University Press, 2011.

[22] **P. Hadfield, S. Lister, P. Traynor.** This town’s a different town today: Policing and regulating the night-time economy. *Criminology and Criminal Justice*, 9(4): 465-485, 2009.

[23] **Victorian Law Reform Commission (VLRC).** *Surveillance in public places final report*, no. 18. Melbourne, 2010. http://www.lawreform.vic.gov.au/sites/default/files/Surveillance_final_report.pdf

[24a] Law, Justice and Safety Committee. *Inquiry into alcohol-related violence, Interim report,* no. 73, Brisbane, Qld: Government of Queensland, 2009.

[24b] Law, Justice and Safety Committee. *Inquiry into alcohol-related violence,* no. 74, Brisbane, Qld: Government of Queensland, 2010. <http://www.aic.gov.au/crime_types/violence/alcohol%20and%20drug%20related%20violence.aspx> [Accessed on 3 June 2010].

[25] B. Bloomfield. In the Right Place at the Right Time: Electronic Tagging and Problems of Social Order/Disorder. *The Sociological Review*, 49(2): 174-201, 2001.

[26] Queensland Government. *Queensland Government Response to Law, Justice and Safety Committee's Report into alcohol-related violence*. Brisbane, Qld. Government of Queensland, 2010. <http://www.parliament.qld.gov.au/documents/committees/LJSC/2009/alcohol-related-violence/responseReport74.pdf> [Accessed on 12 March 2012].

[27] J.T. Cross. Age Verification in the 21st Century. Swiping Away your Privacy. *The John Marshall Journal of Computer and Information Law*, 23(2): 363-410, 2005.

[28] D. Palmer, I. Warren, P. Miller. ID scanning, the media, and the politics of urban surveillance in an Australian regional city. *Surveillance and Society*, 9(3): 293-309, 2012.<http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/aussie_regional>. [Accessed on 30 March 2012].

[29] G.G. Clavell, L.Z. Lojo, A. Romero. CCTV in Spain: An empirical account of the deployment of video-surveillance in a Southern-European Country. *Information Polity*, 17: 57-68, 2012.

[30] M. Tesoriero. Securing our Streets. *Police Life: The Victoria Police Magazine (The Public Safety Edition)*, Melbourne, Vic: Victoria Police Media and Corporate Communications Department, 2010. <www.police.vic.gov.au/retrievemedia.asp?Media_ID=56600>, pp. 8-9. [Accessed on 12 March 2012].

[31] J. Dowling. Police issue record number of banning notices. *The Age*, 26 enero de 2010, <http://www.theage.com.au/national/police-issue-record-number-of-banning-notices-20100125-muhi.html>.

[32] M. O'Brien. Tough new laws to tackle drunken louts. State government of Victoria Media release, 1 March 2011. <http://www.premier.vic.gov.au/wp-content/uploads/2011/03/110301-OBrien-Tough-new-laws-to-punish-drunken-louts-PDF-41KB.pdf>. [Accessed on 12 March 2012].

[33] D. Palmer, I. Warren, P. Miller. ID Scanners in the Australian Night-Time Economy. *IEEE Technology and Society Magazine*, 30(3): 18-24, 2011.

[34] D. O'Connor, W. De Lint. Frontier government: The folding of the Canada-US border. *Studies in Social Justice*, 3(1): 39-66, 2009.

[35] N. O'Brien, E. Duff. You want a drink? Give us your fingerprints. *Sydney Morning Herald*, 30 Jan. 2011. http://m.smh.com.au/entertainment/restaurants-and-bars/you-want-a-drink-give-us-your-fingerprints-20110129-1a8x3.html. [Accessed on 9 March 2012].

[36] D. Murakami Wood. The Surveillance Society: Questions of History, Place and Culture. *European Journal of Criminology*, 6(2): 179-194, 2009.

[37] K. Beckett, S. Herbert. *Banished: The New Social Control in Urban America.* New York, NY: Oxford University Press, 2010.

[38] K.D. Haggerty, R.V. Ericson. The New Politics of Surveillance and Visibility. En *The New Politics of Surveillance and Visibility*, Kevin D. Haggerty and Richard V. Ericson (eds), Toronto: University of Toronto Press, 2006.

[39] W. Bogard. Welcome to the Society of Control: The Simulation of Surveillance Revisited. En *The New Politics of Surveillance and Visibility*, Kevin D. Haggerty and Richard V. Ericson (eds), Toronto: University of Toronto Press, 2006.

[40] Liquor Control Reform Act. Victoria, 1998.

Cristina Blasi Casagran[1], Eduard Blasi Casagran[2]

[1]Researcher at the European University Institute, Florence (Italy); [2]Lawyer at Prodat, Barcelona (Spain)

<cristina.blasi@eui.eu>,
<eblasi@prodatcatalunya.com>

Google: Navigating Security, Rights to Information and Privacy

Abstract: *In the last few years, the rapid development of new technologies and the expansion of the Internet have required multinational businesses to adapt to both national and international laws accordingly.. Thus, companies like Google, Inc. (which today are leading the net) collect and process huge amounts of personal data on a daily basis, without specific legislation to combat the current loopholes in such practices. This study analyses a number of controversial issues related to Google. First, it examines the increase in behavioural advertising, highlighting the potential impact that recent proposals in both the EU and the US could have on this form of advertising. Likewise, it studies the so-called right to be forgotten according to the EU proposal for a General Data Protection Regulation, as well as the impact that this right could have on Google. It then examines the controversy stemming from the blurry dividing line between data collected and processed by private companies (e.g. Google) for commercial purposes, and data processed by public agencies for law enforcement purposes. Finally, the study refers to the new Google privacy policy, which came into force in March 2012. The above areas of inquiry seek to illustrate the enormous power Google has at its disposal with respect to processing internet users' personal data. As such, Google could have a major role in determining global legislative issues such as defining the borders between privacy, rights to information, and collective security.*

Keywords*: Behavioural Advertising, Collective Security, Data Protection, Google, Law Enforcement, Privacy, Right to be Forgotten, Right(s) to Information.*

Authors

Cristina Blasi Casagran is currently a PhD Researcher at the European University Institute (Florence, Italy) on "*The External Dimension of the Area of Freedom, Security, and Justice. Data Protection within the framework of the external relations*". She has previously obtained an LL.M in European Law at Europa Institut (Universität des Saarlandes Germany), an M.A in European Integration at the Institut Universitari d'Estudis Europeus, and a law degree from the Universitat Autònoma de Barcelona. She carried out apprenticeships in the Legal Service of the European Commission, as well as in the Office of the European Data Protection Supervisor.

Eduard Blasi Casagran is a specialised lawyer in data protection and new technologies from Prodat (Barcelona Area, Spain). He is also a member of the Asociacioìn Profesional EspanÞola de Privacidad (APEP) and IT Member in the Sabadell Bar Association. Previously, he worked with the legal service of the Catalan DPA and in the Office of the European Data Protection Supervisor. In addition, he has also done additional postgraduate study on data protection and privacy at the Universidad de Murcia.

1. Introduction: The Internet and the New Concept of Commerce

In the last twenty years, rapid technological change has had a great impact on the creation and proliferation of new forms of commerce. Such commerce is mainly based on knowing as much as possible about each targeted person, so that he/she can be offered a product or service according to his/her preferences and location.

The expansion of the Internet has facilitated the mass collection and storage of personal data. Commercial companies have seen this phenomenon as the best tool to reach the highest number of consumers and as a means to considerably increase their sales.

While users have taken advantage of this fascinating tool (which makes available information from all over the world, enables contact between persons separated by great distances, and simplifies any kind of commercial and recreational operation) companies have found an incentive in acquiring precise information about potential customers online.

The "Internet giants" are behind all of this entire web of interests. These are companies that have been placed in an intermediate position between the interesting information for the user and the attractive data for marketing and advertising companies. They are the Internet search engines.

Today, Google is the search engine *par excellence.* In fact, this company has eclipsed other search engines such as Yahoo Search! or Bing, constituting its own virtual monopoly[1] . But Google is not only the most popular search engine in the net, but also one of the top-three email providers, a social network, and the owner of both Blogger and the biggest video platform online – Youtube [1]. Hence, considering that the main objective of Google is the collection and storage of the greatest amount of data in order to sell this to marketing companies afterwards, Google's competitors are no longer other search engines but the other Internet giants, such as Facebook, Twitter, Microsoft, and Apple.

Accordingly, this study will first examine the impact of the privacy policy that Google adopted on 1 March 2012. After that, the present analysis will look at a few controversial practices resulting from Google's collection and storage of personal data. In particular, it will examine behavioral advertising, the right to be forgotten, and the frequent link between the main Internet companies like Google, with government and law enforcement agencies. This study seeks to highlight some of the main controversial aspects between the massive processing of data from Google (for informational, commercial, or security purposes), and the right to data protection and privacy, according to both future European and U.S. laws.

2. Google's New Privacy Policy

Companies' privacy legislation is mainly adopted through self-regulation, namely, they decide on the privacy clauses that they apply to their users. Companies are entitled to decide which kind of information to take, when cookies will be installed and, in general, the company's privacy standards. In this regard, on 24 January 2012, Google decided to launch a new privacy policy, which came into force on 1 March 2012. This new policy replaces the more than 60 different policies with which Google previously had to comply, and it consists of integrating user data introduced into the net every time a person uses any of Google's platforms: Gmail, Google Maps, Google Apps, Blobber, Chrome, Android, Youtube and Google+, among others.

In terms of the EU's legal framework, the new privacy policy is being reviewed by the DPA of the various member states[2], which unsuccessfully asked to postpone the change in policy coming into force until it could have been properly examined and determined that it did not clash with European and national laws. However, Google justified the rush in

> "Likewise, eight members of the US Congress sent a letter to Google, in which they asked for more information related to the change of its privacy policy"

adopting its policy as being necessary to simplify its services, as well as to improve users' experience every time they use its platforms[3] .

After the *Commission National de l'Informatique et des Libertés* (CNIL) sent Google an 18-page letter requesting the above postponement, together with an extended annex of 69 questions on its effects[4] , Google answered on 5 April maintaining that its privacy policy was completely legitimate[5] .

In the United States, numerous debates have stemmed from the adoption of the new policy. The Electronic Privacy Information Center (EPIC) lodged a complaint against the Federal Trade Commission (FTC) before the federal court with the aim of pushing the FTC to act against such policy[6] . However, on 24 February 2012, the federal court dismissed the complaint stating that there was insufficient evidence to prove that Google's privacy policy conflicted with relevant US law[7] .

Likewise, eight members of the US Congress sent a letter to Google, in which they asked for more information related to the change of its privacy policy[8] . Further, the National Association of Attorneys General sent a letter expressing its discomfort with the new policy, since the consumer is forced to provide information to Google without offering an opt-out possibility. The Association also regretted that Google does not inform its users that the profiling, collection and storage of their personal data may affect their privacy [2].

As for the complaints lodged by citizens, there are currently many lawsuits brought by Google users before the U.S. courts claiming infringement of the previous policies. They argue that those policies guaranteed that the information updated by the user would not be used for other purposes unless the user gives his/her consent [3], and they argue that such clauses have not been respected.

Thus, Google's new privacy policy is having many implications within the privacy sector, since it has become the largest database to date, ahead of its rival Facebook. Consequently, it is still too early to determine what are the uses and limits in the processing of its data. However, an uncontrolled use of this data could turn into the most dangerous weapon against the fundamental right to data protection—an outcome which the EU is tring to prevent. Nevertheless, Google's new privacy policy would not be so controversial if it did not lead to practices such as the promotion of behavioral advertising, difficulties in being forgotten on the net, and the frequent passing of data to public agencies for law enforcement purposes. The next section will analyse each of these aspects from a legal perspective.

3. The Legitimacy of Google within and beyond the EU

Google has put at users' disposal all the information they could possibly ever require. However, this information often includes personal data, and this is responsible for several tensions between the right to be informed and an individual's right to data protection. To be clear, the right to data protection, the right to information, and the right to collective security are not absolute rights. Therefore, this section will examine how these rights interact with Google's practices, and how this search engine, due to current legal loopholes, has often sacrificed the right to data protection for the benefit of government and commerce.

3.1. Behavioural Advertising

For many years now, we have been victims of monitoring systems, which have been collecting everything about what we search on the Internet and, surprisingly, it has often been done without our consent (e.g. Google Trends or, more intrusively, the content filters used by Gmail in order to provide personalised advertisements).

Google is and has been one of the main leaders on the Internet in behavioural advertising (alongside Microsoft, Yahoo, Apple, and Facebook). Thus, through so-called "cookies", which are tiny files installed on a user's computer, Google controls users' activities over the Internet, as well as their preferences, tastes and interests. This data is then sold to advertising and marketing industries. For instance, in Minneapolis a man found out that his teen daughter was pregnant when he received baby food and clothes coupons sent to his home by a department store. The girl had not subscribed to that department store's mailing list, but she had been identified by a system which detects pregnant women's profiles via their purchases [4] .

In order to avoid situations like the one above, the user occasionally has the possibility to request an opt-out from the website. In other words, the user is able to expressly reject these kinds of personalised advertisements, but here is where the controversy arises. In the United States, this model of opt-out advertisements saw the light of day in 1997 from the Clinton Administration, when the expansion of e-commerce was starting, and it allowed industries to self-regulate their behavioural advertising and their cookies.

However, within the EU legal framework, the user's prior consent is required before installing cookies in the browser as per e-Directive 2009[9] . In particular, article 5(3) of the directive states that: "*Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC […]*". Hence, the directive set up a system of opt-in (and not opt-out) among member states, which was to be implemented on 25 May 2011 at the latest. Spain has recently transposed the directive through the Spanish Royal Decree 13/2012[10] , which, as of 1 April 2012, has modified former Spanish legislation on telecommunications. Article 22(2) of the decree introduces the requirement of consent by user's express action, which must be also prior and informed. This new requirement increases users' control, and in particular, that they may accept or reject the installation of cookies every time they use the Internet.

Accordingly, two big European advertising companies, EASA and IAB, have published "Recommendations on Best Practices" on April 2011[11] . These initiatives were supported by the Vice-president of the Commission Kroes [5], but they were not welcomed by the Article 29 Data Protection Working Party (hereinafter, Art.29WP), which announced that it would launch a survey on codes of conduct within the field of behavioural advertising in order to establish a basis for the self-regulation system[12] .

Recently, two big events have taken place, which could have consequences in the field of behavioural advertising. First, the European Commission published a Proposal for General Data Protection Regulation on 25 January 2012; and second, the Obama Administration launched the Guidelines on Consumer Privacy Bill of Rights on 23 February 2012[13] .

On the one hand, article 3(2) of the Regulation establishes that "*This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller*

> “ The Russo case is only one of numerous current cases in which both the Data Protection Authority’s (DPAs) and users can be seen as powerless in terms of removing users’ personal data from the net ”

not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour". In other words, Google would be subject to the Regulation through this extraterritorial clause. Thus, every time Google creates profiles by collecting personal data, the company would have to comply with article 20 of the Regulation. Paragraph 2(c) of article 20 refers to the requirement of consent, which has to be specific, informed and explicit[14] (article 4(8) of the Regulation).

On the other hand, the US Guidelines on the Privacy Bill of Rights opt for a legislative procedure which allows the participation of private sector (including Google) during the drafting of future codes of conduct. The report also refers to the so-called Do-Not-Track (DNT) rules, by which consumers are able to block data collection from Internet companies. In this regards, Mozilla browser already applies DNT technology in its software [6] and it seems that the Digital Advertising Alliance, which includes companies such as Google, which is willing to introduce this technology in the future. However, this alliance has already announced that DNT will only be possible for advertisments focused on a specific sector [7], so even if users’ requests on not being included are taken into account, there will be cases in which these companies will be allowed to keep collecting behavioural data for a variety of purposes [8] (for instance, in the case of the social network Google+, by the option Google+1).

Therefore, it seems that the flexibility of the system proposed by the US could clash with the more rigid legal framework launched by the EU, as regards the requirements for processing behavioural data. The problem is that global enterprises such as Google are more attracted to the US proposal, since it is more flexible, and this could push the EU to make its proposal softer, in order to bring it closer to the US legal approach.

For all that is said above, the tension between both legal orders could be solved through a project launched by Kroes consisting of creating DNT global standards as part of its programme, Digital Agenda for Europe [9]. However, it remains to be seen to what extent companies like Google will influence the drafting of those standards, as well as their efficiency in protecting users’ personal data.

3.2. The Right to be Forgotten

Thanks to Google, users today have access to all kinds of information, from news stories to official documents (even confidential ones). Companies have found on the net an effective way to advertise while users are online, regardless of the user’s location.

However, legal conflict arises when the right of freedom of expression and the right of information (article 20 of the Spanish Constitution) can undermine other fundamental rights, such as the right of data protection and privacy (article 18 of the Spanish Constitution). This was precisely what happenned to Dr. Guidotti Russo, a plastic surgeon who was mentioned in a critical article published by the Spanish journal, *El País* in 1991. The article reported on the legal dispute between Russo and a former patient. The controversy emerged from the fact that Russo, still working as a surgeon today, wanted that article to be removed from Google’s search engine, since everytime someone typed his name into the search engine, the *El Pais* article was ranked in the top positions. This negative publicity caused Russo great financial loss to his practice. Despite the Spanish Data Protection Authority’s (DPA) dispute with Google over removing this article from the search results, the link to the controversial article is still available online today[15].

The Russo case is only one of numerous current cases in which both the DPAs and users can be seen as powerless in terms of removing users’ personal data from the net[16]. In fact, all European citizens have the right of access to the data the entity collects about them[17]. However, paradoxically, the information Google possesses about its users cannot be discovered by applying the right of access (unlike Facebook, as the Austrian student Mark Schrems let as know) [11]. This was the position of Google UK when it was asked to provide all personal data of one of its users. The company said that Google UK did not process any personal data in relation to the search engine, but that it was processed by Google Inc. instead. It is worth highlighting that Google Inc. is governed by US laws, which do not offer the possibility of invoking the right of access to users’ own personal data [1].

In order to improve the situation where the individual remains powerless to access, modify, or delete his/her personal data on the Internet, the Proposal for General Data Protection Regulation has introduced in article 17 a new concept called "the right to be forgotten". It consists of enabling users to permanently delete personal data that they no longer wish to be published on the net. The right to be forgotten, thus, seeks to go beyond the right of erasure established in article 12 of Directive 96/46/EC, or in the same way, the rights of opposition and cancellation as stated in articles 16 and 17 of the Spanish LOPJ[18].

This new right is perceived as a threat to companies such as Google, which have been able to abstain from the rights of opposition and cancellation to date because of a current loophole for Internet search engines. In this respect, Google has argued that *"the information obtained through its search results belong to third-party webpages, whose access is public*" and in order to delete the content of such webpages "*the information should disappear from the webmaster of that third-party’s webpage*"[19]. Besides this, in Europe, Google has tried to escape from legal constraints in this area, arguing that it is the only company that allows its users to send any complaint or suggestion related to the service it offers[20].

The Vice President of the European Commission Viviane Reding has already clarified that in information societies the information society services, such as Google, or social networks shall control the content, conditions and methods of processing of personal data.

In other words, Reding seeks to impose a duty on information society services to act as data controllers. However, she admits that the posting service should also carry out an important role, such as informing the search engine that a user wants his/her data to be removed [12].

With regard to the future responsibility of search engines, Google could get penalties up to the 2% of its annual incomes if it does not delete pictures or other data that an individual has uploaded, but then later wants to remove [13]. This is the reason why the proposal launched by the European Commission has caused a debate among multinational technology companies with branches in Europe. They have argued that the establishment of the right to be forgotten within the EU could jeopardise more than 15,000 millions of Euros of business in the global economy [14].

Likewise, Google’s privacy lawyer distinguished in his blog the difference between services storing data uploaded by the user

> It is a fact that Big Data offers unquestionable advantages, but a balance between the right of information and collective security on the one hand, and the individual rights of *habeas* data on the other, is needed

(e.g., Facebook and Youtube) and services providing personal information existing in another webpage (e.g., Google, Bing or Yahoo!). In the latter case, hosting services and not search engines should be the ones entitled to delete personal information. Thus, Google states that search engines only catalogue the available information, but they do not have any direct link with the original content[21].

Moreover, one of the problems emerging from this new concept of the right to be forgotten is deciding what will happen with the subsequent copies of personal data, which remain once the original information has been deleted. Accordingly, Reding has already clarified that only in cases where the data controller has authorised the publication of personal data to a third party, will it be considered responsible for such publication [15].

Finally, it is worth highlighting the potential clash between the right to freedom of expression (as conceived by the US Supreme Court) and the right to be forgotten. Even though the proposed EU regulation predicts a number of exceptions on the enforcement of the right to be forgotten in order to protect the freedom of expression (article 17(3) of the Regulation), the US Supreme Court has expressed that the States are not empowered to adopt legislation that restricts communications (censorship in other words), not even in cases of embarassing information (e.g. the name of a raped person), as long as this information is collected using legitimate means [13]. But the unanswered question is: What if the victim wants this information to be removed?

3.3 Link with Public Authorities

Together with the right of information and the right to data protection, the right to collective security has had implications regarding the activities Google has carried out in the last ten years. In fact, the line dividing the processing of personal data by public and private entities is becoming increasingly blurred. Originally, the division was clear: private companies collected data for commercial purposes; and government and police authorities processed data with the aim of preventing or fighting crime. However, the rise in international terrorism today has required private companies to provide law enforcement with users' personal data for counter-terrorist purposes[22].

Google has admitted that it has given users' information to the US government, since according to 1986 Electronic Communications Privacy Privacy Act, neither court order nor prior notification to the user are required [16]. Likewise, since 9/11 attacks, the USA Patriot Act allows the US authorities to require any kind of personal information collected by private companies during a counter-terrorism investigation.

With the purpose of reducing users' insecurity about not knowing where their data is processed, Google created the Transparency Report[23], which allows users to see the number of governmental requests for their data, as well as the information blocked by governments. The report is classified by semesters and according to the country.

The Transparency Report illustrates how private companies such as Google are gaining important roles in the collection and processing of personal data, since they do not only provide data to other private companies for advertising purposes, but also to the government with the aim of creating profiles of criminal suspects[24].

It is a fact that Big Data[25] offers unquestionable advantages, but a balance between the right of information and collective security on the one hand, and the individual rights of *habeas* data on the other, is needed [7]. The frequent practice of governments to seize massive amounts of data (not only from suspects or criminals) for security purposes is controversial: Where is the limit? Is the intrusion presumptively proportional and justified as long as it is for "counter-terrorism purposes"? The popular argument "I have nothing to hide"[26] shows the priority of collective security over individual privacy. However, more privacy should not imply less security or vice versa [19], but the key issue is to strike the right balance between both rights.

4. Conclusions

As The New York Times stated, personal data is the fuel of the twenty-first century [20]. Massive technological advances, globalisation of markets, and the enhancement of counter-terrorism measures, are some of the major factors driving the mass collection and processing of personal data, from both public and private entities.

Specifically, this study has analysed the way Google processes personal data in the current digital era. It examined the privacy laws and potential clashes between the EU and the US legal approaches, as well as the limits of responsibility in the processing of personal data. Likewise, new phenomena such as the right to be forgotten or behavioural advertising have been examined, focusing on the EU attemps to safeguard the fundamental right to data protection.

The study has also looked at some controversial data protection issues that have emerged due to the expansion of the most popular search engine, Google, which has vowed to fight where opposing viewpoints clash: First, the right of information and freedom of speech; second, the collective security in a world invaded by terrorism and criminality; and third, the duty to protect personal data and individuals' privacy, whose data are constantly collected and processed by private and public actors.

As stated above, it can be concluded that Google has acquired the title of "emperor" on the net, becoming the main obstacle for the DPAs within the EU. Google represents the new digital era, where the power is measured by the control a company has on the net. Despite the US and EU lawmakers' efforts to get both legal approaches closer and removing the current loopholes on privacy and data processing, there is still a long ways away.

Maybe, one day we will be able to speak about global standards on data protection as proposed in the Madrid Declaration in 2009, considering that data protection is already part of all current legislative agendas. Now it remains to be seen to what extent companies such as Google are involved in the decision making, and how it could affect to the protection of our personal data.

References

[1] J. Ball. "Me and my data: how much do the internet giants really know?", *The Guardian*, 22.04.2012. <http://www.guardian.co.uk/technology/2012/apr/22/me-and-my-data-internet-giants?fb=native>.

[2] S. Forden. "Google Privacy Policy Criticized by State Attorneys General", *Bloomberg.com,* 22.02.2012. <http://www.businessweek.com/news/2012-02-22/google-privacy-policy-criticized-by-state-attorneys-general.html>.

[3] J. Ribeiro. "Google faces class action lawsuits against new privacy policy", *Computer World*, 22.03.2012. <http://www.computerworld.com/s/article/9225406/Google_faces_class_action_lawsuits_against_new_privacy_policy?taxonomyId=17>.

[4] C. Duhigg. "How Companies Learn Your Secrets", *The New York Times*, 16.02.2012. <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&pagewanted=all>.

[5] N. Kroes. "*Towards more confidence and more value for European Digital Citizens. European Roundtable on the Benefits of Online Advertising for Consumers*". SPEECH/10/452. Brussels, 17.09.2010.

[6] A. Fowler. "Mozilla Led Effort for DNT Finds Broad Support". *Mozilla Privacy Blog. Covering the latest developments in privacy & data safety*, 23.02.2012. <http://blog.mozilla.com/privacy/2012/02/23/mozilla-led-effort-for-dnt-finds-broad-support/>.

[7] E. Mills. "Firms embrace Do Not Track for targeted ads only", *CNET News*, 23.02.2012. <http://news.cnet.com/8301-31921_3-57384193-281/firms-embrace-do-not-track-for-targeted-ads-only/>.

[8] R. Waters. "Europe and US to clash over online data protection", *Financial Times*, 23.02.2012. <http://www.ft.com/intl/cms/s/0/c039ce50-5e4b-11e1-85f6-00144feabdc0.html#axzz1nLUCGPgH>.

[9] N. Kroes. "*Why we need a sound Do-Not-Track standard for privacy online*", enero 2012. <http://blogs.ec.europa.eu/neelie-kroes/donottrack/>.

[10] V Mayer-Schönberger. "*Delete. The Virtue of Forgetting in the Digital Age*". Princeton University Press, New Jersey, 2009. ISBN-10: 0691138613.

[11] B. Donohue. "Twenty Something Asks Facebook For His File And Gets It - All 1,200 Pages", *Threat Post*, 13.12.2011. <http://threatpost.com/en_us/blogs/twenty-something-asks-facebook-his-file-and-gets-it-all-1200-pages-121311>.

[12] T. Espiner. "Firms face tough new EU fines for data breaches", *ZDNet UK*, 25.01.2012. <http://www.zdnet.co.uk/news/security-management/2012/01/25/firms-face-tough-new-eu-fines-for-data-breaches-40094907/>.

[13] J. Rosen. " The right to be forgotten", *Stanford Law Review*,13.02.2012. <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>.

[14] S. Sengupta. "Facebook's Sandberg Gently Warns Europe About Privacy Rules", *The New York Times*, 24.01.2012. <http://bits.blogs.nytimes.com/2012/01/24/facebooks-sandberg-gently-warns-europe-about-privacy-rules/>.

[15] D. Meyer. "EU puts Google straight on "right to be forgotten", *ZDNet UK,* 22.02.2012. <http://www.zdnet.co.uk/news/security/2012/02/22/eu-puts-google-straight-on-right-to-be-forgotten-40095097/>.

[16] J.P. Titlow. "Google Hands Wikileaks Volunteer's Gmail Data to U.S. Government", *ReadWriteWeb*, 10.10.2011. <http://www.readwriteweb.com/archives/google_hands_wikileaks_volunteers_gmail_data_to_us.php>.

[17] A. Krotoski. "Big Data age puts privacy in question as information becomes currency", *The Guardian*, 22.04.2012. <http://www.guardian.co.uk/technology/2012/apr/22/big-data-privacy-information-currency?newsfeed=true>.

[18] Daniel J. Solove. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy", *San Diego Law Review, Vol. 44*, p. 745, 2007.

[19] Adam D. Moore. "Privacy, security and accountability", Chapter 10 of "*Privacy Rights. Moral and Legal Foundations*", The Pennsylvania State University Press, USA, 2010.

[20] J. Brustein. "Start-Ups Seek to Help Users Put a Price on Their Personal Data", *The New York Times*, 12.02.2012. <http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html?_r=3>.

Notes

[1] In fact, the European Commission has an investigation open since November 2010 for an alleged violation of Art. 102 TFEU for an abuse of a dominant position. <http://europa.eu/rapid/press-release_IP-10-1624_en.htm>.

[2] Letter from the Article 29 Data Protection Working Party to Google Inc, 02.02.2012. <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf>.

[3] Letter from Google to the Commission Nationale de l'Informatique et des Libertés (CNIL), 03.02.2012. <http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf>.

[4] CNIL, Ref. IFP/BPS/CE121169. <http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf>.

[5] Google defends privacy policy to European watchdog, 05.04.2012. <http://www.reuters.com/article/2012/04/05/google-privacy-idUSL6E8F5ASO20120405>.

[6] <http://epic.org/privacy/ftc/google/EPIC-Complaint-Final.pdf>.

[7] <http://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf>.

[8] Letter from the US Congress to Google, 26.01.2012. <http://www.reuters.com/article/2012/01/26/us-google-privacy-idUSTRE80P1YC20120126>.

[9] OJ L337, 18.12.2009, p.11-36. This directive amends the previous Directive 2002/58/EC (ePrivacy), OJ L2012, 31.7.2002, p.37-47. - Note from the reviewers: *It should be noted that not all countries have enacted legislation on this including Germany*.

[10] BOE (Spanish Official State Gazette) 31 March 2012, num. 78, sec I.P 26876-26967.

[11] EASA Best Practice Recommendations on Online Behavioural Advertising. Setting out a European advertising industry-wide self-regulatory standard and compliance mechanism for consumer controls in Online Behavioural Advertising", 13 April 2011; European Self-regulation for Online Behavioural Advertising. Transparency and Control for Consumers, IAB Europe, 27 April 2011.

[12] Press release Article 29 Data Protection Working Part, 15.12.2011.

[13] <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

[14] For a more exhaustive definition of these terms, see Opinion 15/2011 on the definition of consent, WP187, 13.7.2011.

[15] El Paìs, 28.10.1991, <http://elpais.com/diario/1991/10/28/sociedad/688604403_850215.html>.

[16] For an exhaustive study regarding the right to be forgotten in the digital era, see [10].

[17] Art. 12 of the Directive 95/46/EC.

[18] BOE nuìm. 298, 14.12.1999. *Ley Orgaìnica 15/1999*, 13 December 1999, on Personal Data Protection.

[19] AEPD, SP/SENT/626428, 320/2008, 7 April 2011.

[20] "Our thoughts on the right to be forgotten". Google European Public Policy Blog, 16.02.2012 <http://googlepolicyeurope.blogspot.com/2012/02/our-thoughts-on-right-to-be-forgotten.html>.

[21] "Our thoughts on the right to be forgotten". Google European Public Policy Blog, 16.02.2012 <http:// googlepolicyeurope.blogspot.com/2012/02/our- thoughts-on-right-to-be-forgotten.html>.

[22] This is the case of PNR agreements, by which airline companies provide passengers' data to the US, Canadian and Australian authorities; or SWIFT agreement, by which this entity send financial data of EU citizens to the US authorities. Both agreements have its rationale in preventing and combating terrorism.

[23] <http://www.google.com/transparencyreport/governmentrequests/userdata/>.

[24] For exemple, the NY police used a picture on Facebook combined with its own pictures files and a facial recognition program to arrest a man suspected of murder. <http://rt.com/usa/new-york-barbershop-shooting-951/>.

[25] For a definition of this term, see <http://mike2.openmethodology.org/wiki/Big_Data_Definition>.

[26] See the debate behind this argument in [18].

Fernanda Glória Bruno[1], Liliane da Costa Nascimento[1], Rodrigo José Firmino[2], Marta M. Kanashiro[3], Rafael Evangelista[3]

[1]Federal University of Rio de Janeiro (UFRJ), Brazil; [2]Pontifícia Universidade Católica do Paraná (PUCPR), Brazil; [3]State University of Campinas (Unicamp), Brazil

<bruno.fernanda@gmail.com>, <liliane.line@gmail.com>, <rodrigo.firmino@pucpr.br>, <mmk@unicamp.br>, <rae@unicamp.br>

Human Traces on the Internet: Privacy and Online Tracking in Popular Websites in Brazil

Abstract: *The Internet has made our actions and lives increasingly traceable. Data about our habits, preferences, tastes and interests can be easily collected, stored and processed on the web, which has an inestimable value to several private parties interested in predicting our online and offline behaviors. This paper aims to shed some light on how this data collection takes place in popular websites in Brazil. In order to do so, we investigate tracking mechanisms used in five websites and two social network websites. We identify the HTTP cookies, Flash cookies and web beacons used in each of them. The trackers are analyzed in quantitative and qualitative terms, based on the practices of the companies responsible for operating them. Based on that, we discuss the contributions and limitations on the notion of privacy related to the use of trackers in the Brazilian context.*

Keywords: *Brazil, Cookies, Online Marketing, Online Tracking, Privacy, Web Beacons.*

Authors

Fernanda Glória Bruno is an Associate Professor in the graduate program in Communication and Culture at the Federal University of Rio de Janeiro (UFRJ), Brasil. She has a PhD in Communication from the Federal University of Rio de Janeiro (Doctoral Research Fellow at Paris Descartes University, Sorbonne, 2000). She is also a National Counsel of Technological and Scientific Development/CNPq researcher and founding member of the Latin America Network of Surveillance, Technology and Society Studies. In 2010-2011 she was a visiting researcher at Sciences Po (CERI and Médialab), Paris (France).

Liliane da Costa Nascimento is a PhD Candidate in Communication and Culture at the Federal University of Rio de Janeiro (UFRJ), Brasil. She holds a master's degree from the same university. Her researches interests include surveillance technologies, cyberculture and social control. She is a member of the Latin American Network of Surveillance, Technology and Society Studies.

Rodrigo José Firmino is a lecturer in the Postgraduate Program of Urban Management at the Pontifícia Universidade Católica do Paraná, in Curitiba, Brazil. Rodrigo is also a CNPQ Research Fellow. He worked as a Postdoctoral Fellow at University of São Paulo, Brazil, researching the co-development of urban and technological strategies for cities in developing countries. He obtained his Ph.D. on Urban Planning from the School of Architecture, Planning and Landscape at the University of Newcastle upon Tyne, U.K. He also holds an MPhil in Architecture and Urbanism from the University of São Paulo, and trained as an architect and planner at State University of São Paulo. Rodrigo is one of the founding members of the Latin American Network of Surveillance, Technology and Society Studies.

Marta M. Kanashiro is a professor in the Postgraduate Programme in Scientific and Cultural Communication at the University of Campinas (Unicamp), Brazil. Marta is also a researcher in the Laboratory of Advanced Studies on Journalism and in the research group Knowledge, Technology and Market (CTeMe), both in the same university. She obtained his Ph.D on Sociology in University of São Paulo (USP) and his main interests focus on Science Communication and Sociology of Technology from a critical perspective on new developments in science or new technologies. She has been studying surveillance technologies in Brazil, since 2001. Her research includes an investigation about the use of CCTVs in the city center of São Paulo (2002-2005) and the use of biometrics in the Brazilian Id Card (2007-2011). She is a Founding member of the Latin American Network of Surveillance, Technology and Society Studies.

Rafael Evangelista is a professor in the Postgraduate Program of Science and Cultural Communication an a researcher in the Laboratory of Advanced Studies on Journalism at the State University of Campinas (Unicamp), Brasil. He holds a Ph.D in Anthropology and an MPhil in Linguistics both from Unicamp. His main research interests and publications are on the cultural and social aspects of Internet and network society, free and open source software communities, commons-based peer production, and science communication. He is a Member of the Latin American Network of Surveillance, Technology and Society Studies.

1. Introduction

The intensive monitoring and data gathering of people's online activities is the core element of a new business model for the Internet, in which we pay for information and services offered as if they were for free with personal information [1]. These data, collected throughout the Internet as we navigate from website to website, are successively stored, processed, and then (as it is claimed by the tracking industry) used to predict our future behavior as consumers and deliver us tailored advertisements. These processes have remained largely oblivious to Internet users, who usually do not know when or by whom their information is being collected, nor to which purposes it will be used.

This everyday monitoring of peoples' ways of life has given rise to a series of debates about privacy. It is known that several forces are driving changes in the meaning, practices, contours and experience of privacy on different levels: conceptual, commercial, political, social, subjective etc. These processes are not homogeneous and in some cases, they have been happening in spite of actors' consciousness about its reach and complexities. In this context, abstract definitions of privacy do not allow us to grasp what is at stake [2][3]. We consider it essential to observe and identify, from a sociotechnical perspective [4], the actions and practices through which this renegotiation has been performed.

This paper aims to contribute to this approach, by focusing on a specific field of practices and monitoring technologies related to online activities in Brazil. It presents the results of a preliminary survey whose main objective is to reveal and discuss how online tracking is taking place in seven websites ranked among the most visited by Brazilians.

Therefore, we start by briefly presenting the general framework of online tracking, with its activities of data gathering and processing. Hereupon, we present the survey methods and results. Then, we situate public debate and regulatory framework on privacy and data protection in Brazil and finally, we raise privacy questions related to the subject of control over personal information.

> "Through this process, which is opaque to the great majority of users, companies can place small files at visitors' computers and track their web surfing activity over time and across sites"

2. The Growing Value of Personal Information

While in the offline world data gathering is frequently related to a single domain or activity, on the Internet any action can be traced. Over time, it has enabled huge databases to emerge, containing data about almost any aspect of people's lives. The question then becomes how to cope with this large amount of information and extract value from it, which has been answered with the emergence of sophisticated computational and statistical technologies.

The consumer profiling industry is largely based on methods such as profiling and Knowledge Discover in Databases (KDD), also called Data Mining (DM). In short, they enable scouring databases for hidden patterns without the need to draw from hypothesis formulated by a human being [5].

In general, databases can be analyzed in two main ways, each one having different privacy implications. Descriptive practices consist of scanning the data available to retrieve information about the database as a whole. Predictive tasks, in their turn, enable the making of guesses about a future condition. Once analysts have segmented their databases, they claim that they become able to anticipate the future conduct of the individuals previously classified, or predict the behavior of others about whom they have almost no information.

As it is well known, the Internet works based on a constant exchange of information – users are always sending requests to the websites they access and downloading data from its host servers. Through this process, which is opaque to the great majority of users, companies can place small files at visitors' computers and track their web surfing activity over time and across sites. These pieces of software, called cookies, collect the information that will enable behavioral targeting and influence the advertisements one sees when visiting a website. Other trackers, such as web beacons, can also be used to this purpose[1].
What our clicks can reveal is attached to the content available on the website we visit[2].

Thus, the knowledge about individuals is restricted and no single entity collects all personal information on the web. It drives efforts to collect data across websites, using cookies and also other tracking methods[3]. As Peter Eckersley argues, "*the core function of the cookie is to link what you do on Web site A to what you do on Web site B*" [11].

In the online market case, it is done by ad networks, which manage the placement of advertisements in a group of websites. Advertisements are not stored in the publisher's server, but in an ad server, which delivers the advertisements to the websites visitors[4] are seeing. It enables companies to track our online habits and preferences through different and not related websites, which has important privacy implications[5].

3. Data Collection and Tracking in Brazilian Websites

There are several reasons to look at online tracking in Brazilian sites. Brazil has the largest online population in Latin America. Worldwide, it is the eighth country in number of Internet users. According to a survey carried out in 43 countries [12], there are 41.5 million active Brazilian users[6], who spend, in average, 24.3 hours online per month, 2 hours more than the global average. In addition, online population in Brazil has grown by 19% from March 2010 to March 2011, a number 8% bigger than the increase of worldwide online population in the same period.

Two statistics brought out by this research are of particular interest to the purposes of this article. The first one shows that the habit of online purchasing is becoming more popular among Brazilians, which moves tracking industry forward. In December 2010, 69.6% (seven out of ten Brazilian users) visited retail websites, a rate that is the highest in the region. A comparison with the same month in 2009 shows a 9% growth. The second statistic we highlight is about social networking usage. Brazil is the fifth largest social networking population in the world, and social network reach in the country is 85.3%, 14.8% higher than the worldwide average. According to another research, the usage of social network websites is the third biggest online activity for users in Brazil [13].

Following these data, we have examined two social network websites (Orkut and Facebook[7]) and five websites listed among the fifteen most visited in the country[8] (Terra[9], UOL[10], Globo.com[11], Yahoo!Brasil[12] and YouTube[13]). We have looked for HTTP cookies, Flash cookies and web beacons used in each of them and analyzed the trackers found in quantitative and qualitative terms, based on the practices of the companies responsible for their operation.

4. Methods

The data for this survey were collected in February 2010[14]. The methodology employed has been partially drawn up from an analysis conducted by The Wall Street Journal [14] and varies according to the kind of trackers analyzed.

The search for HTTP cookies was done basically in three steps: (1) by deleting all web browser's cookies; (2) by visiting, on average, 30 different pages in each domain; (3) and finally, checking the HTTP cookies stored in the web browser. Flash cookies analysis followed a similar method, but since these trackers are not stored in the web browser, we used Adobe Flash Player: Settings Manager[15], an Adobe Panel controlled via webpage that shows a list of domains storing flash content in a computer. At last, to conduct the web beacon's examination, we used Gosthery[16], a browser tool that notifies the user about the presence of web beacons and gives information about companies operating them. During the process, we never logged in and always took care not to access external links.

In social network websites, we examined five social applications in each website, chosen according to their popularity[17]. It is worth mentioning that, in this case, we conducted our analysis logged in as registered users. However, since motivations to track can decrease once you are identified to the system, we focused on these external trackers operated by social platform developers or companies working for them.

After their identification, we analyzed each cookie domain, in order to know which company had set them. Sometimes, the domain's name gave us this information, but when it was not explicit, we had to search for it using Robtex[18], a tool that provides domain name consulting. Then, we visited each company's website to learn about the service it provides. We also searched for their privacy policies and checked if they offered an opt-out mechanism for their trackers. Based on this information, we classified the trackers found.

5. Results

On the five websites analyzed, we have found a total of 334 HTTP cookies (see **Figure 1**) (174 set by third parties and 53 set by different domains), 3 Flash cookies and 25 web beacons (considering only the exclusive ones). The examination of trackers distribution across sites has revealed that the number of third party HTTP cookies found on Terra,

> “ After their identification, we analyzed each cookie domain, in order to know which company had set them ”

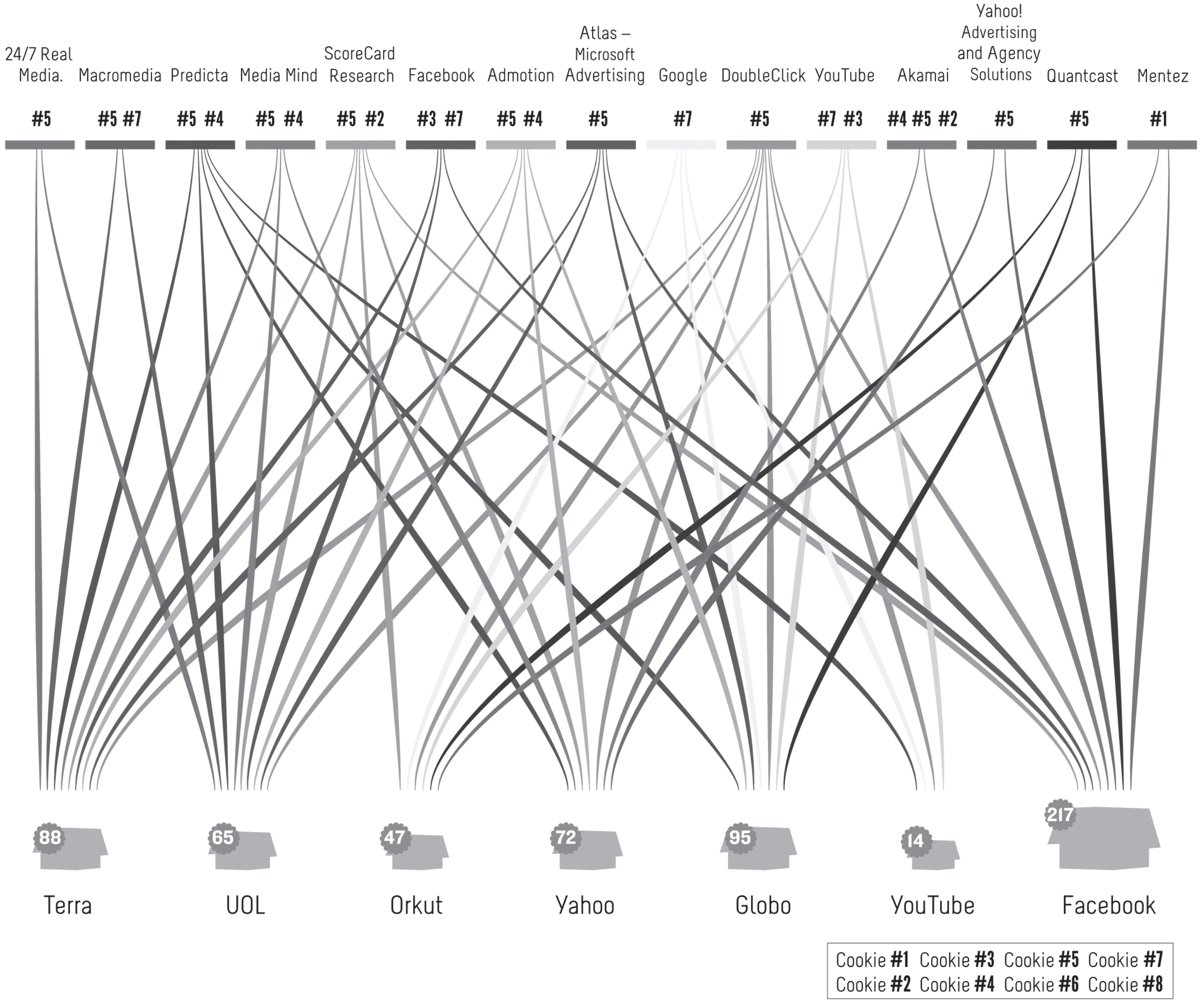


Figure 1. Characteristics of the Most Common HTTP Cookies, the Websites Where They Were Found and the Companies that Set Them[19].

UOL and Yahoo is 4.2 times bigger than the number of cookies found on Globo.com and YouTube. When it comes to web beacons, UOL and YouTube have used less trackers of this type (1 and 3, respectively) than Yahoo, Terra and Globo.com (which have set 6, 7 and 8 web beacons, respectively).

We also examined these five websites' privacy policies to understand how privacy is considered and informed to the public in these documents. Except for UOL, all policies mentioned that cookies from third parties are allowed. In these cases – all policies observed – data collection and use is governed by the partners' policies. This claim resounds as an attempt to reallocate responsibility, putting on users' shoulders the obligation to analyze all "chain of policies" and take a stand in each situation. Given the expressive number of external cookies revealed by our survey, and how obscure this process may be, we can consider this practice as a source of privacy concerns. On the one hand, the user is charged with the responsibility and work to manage its own privacy. On the other hand, there is no guarantee that he/she can count on the required transparency to negotiate privacy in an autonomous way.

Almost all policies have also emphasized that cookies do not collect personal information and that companies can share aggregated data with commercial partners. In fact, this perspective can be put in check if we consider that the notion of personal data is being challenged by the fact that digital databases can be easily re-identified through pieces of information other than names [15]. Moreover, the lack of identification, in a traditional sense, of a specific individual, does not prevent consumer's engagement. Even anonymous, databases can be used to classify and influence personal conduct, as well as to sort the opportunities offered to the individuals [16].

Social network websites analysis has revealed an expressive asymmetry in the number of cookies found. On Orkut, we have identified 43 HTTP cookies, while on Facebook, there

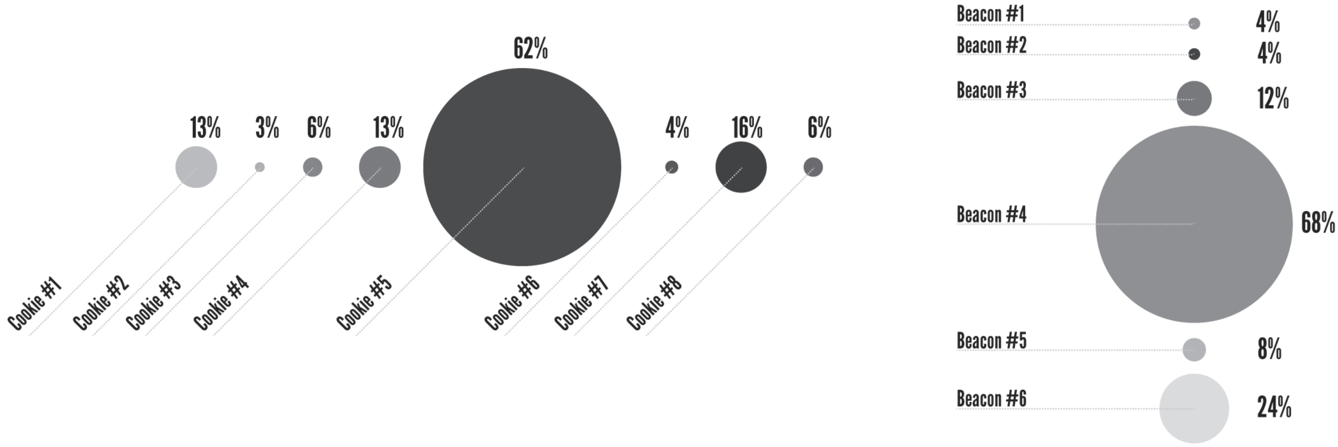


Figure 2. Cookies (on the left) and Beacons (on the right) Ocurrence per Type.[21]

were 217. The number of web beacons, in turn, has ranged from 15 on Facebook to 18 on Orkut (considering only the exclusive ones)[20]. The expressive number of companies operating trackers called our attention. In only seven websites, we identified 69 companies operating cookies and 23 companies operating web beacons. Only four of these companies are located in Brazil: Predicta, Navegg, Zura! and Boo-Box. We also observed the predominance of companies from the online marketing field – 62% of those setting cookies and 68% of those setting beacons provided services such as advertisement serving and optimization (see **Figure 2**). This evidence indicates the importance of discussing and identifying how most parts of personal data storage, monitoring and classification are tied to the dynamics of online marketing.

We have ranked companies responsible for the trackers according to the number of websites in which they appeared (see **Figure 3**). As previously highlighted, the amount of data a company can collect increases with the number of websites in which they deliver advertisements. Doubleclick, Google's branch on online marketing, has set trackers in all websites analyzed and leads the ranking for HTTP cookies, followed by Predicta, a national company which have set cookies in five out of seven websites. Google Analytics, in turn, leads the ranking of web beacons, appearing in all websites analyzed, followed by Google's Ad Sense, which have set web beacons in three out of seven websites.

Our investigation showed that 19% of companies that have set cookies did not offer a privacy policy and 46% did not provide an opt-out option. Among those who operate web beacons, the number of companies that did not offer a privacy policy drops to 4%. We also have found that, among companies that have set beacons, 32% are Network Advertising Initiative (NAI)[22] members, while 56% are certified by TRUSTe[23] or Safe Harbor[24] signatories. Among companies operating cook-

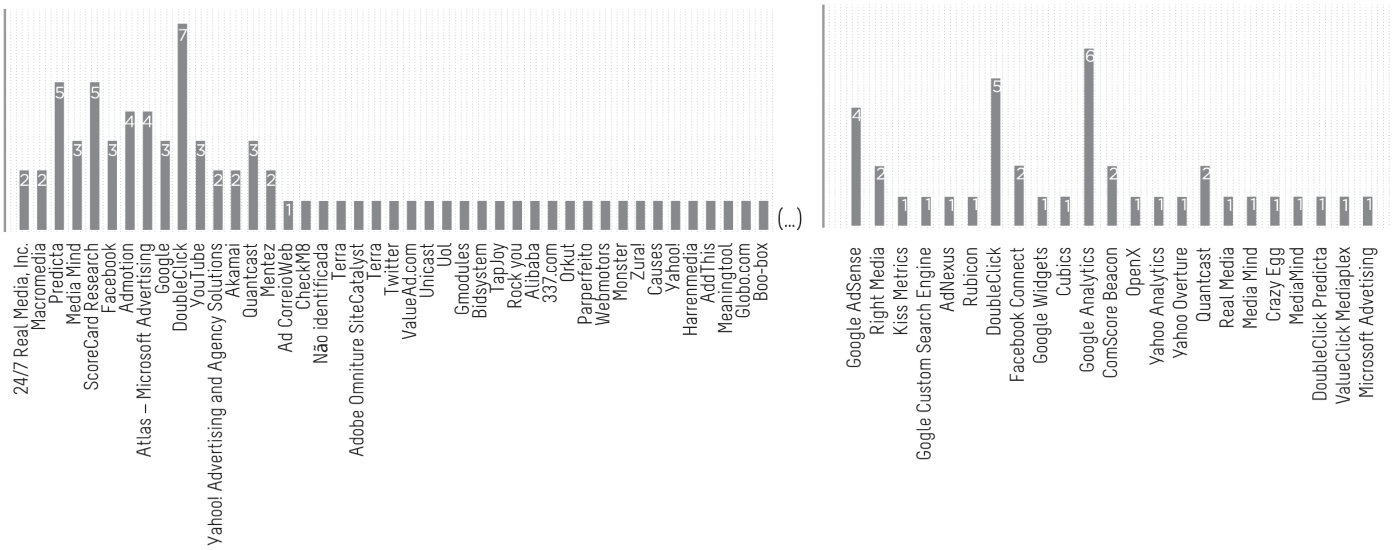


Figure 3. Number of Websites in which We Have Found Cookies (top) and Beacons (bottom) Set by each Company.

> "Social network websites have helped to raise awareness about the reach and visibility of data its users usually post on their profiles, mainly due to Orkut mass adoption in the country"

ies, these numbers drop to 19% and 23%, respectively; 67% of companies operating cookies and 32% of those operating beacons are not NAI, neither TRUSTe nor Safe Harbor signatories.

It is also worth highlighting that, except for a few cases, companies have not been explicit about the usage and opt-out options for web beacons and Flash cookies. In general, their privacy policies employed only the term cookie. Another fact with potential privacy implications, is that, sometimes, the given opt-out mechanism consisted in setting a cookie to indicate the user's option of not being tracked. As this cookie comes from the same domain that trackers cookies came from, it makes the process uncertain concerning the ways companies manage personal data.

6. Public Debate and Regulatory Framework

Despite all tracking evidences discussed above, public debate about online privacy in Brazil is still incipient. Social network websites have helped to raise awareness about the reach and visibility of data its users usually post on their profiles, mainly due to Orkut mass adoption in the country. However, institutional audiences and issues like behavioral targeting, data collection and process have been out of agenda, except for a few cases which gained some relevance and media coverage in the country.

In 2010, Velox and Speedy, well known Brazilian Internet service providers, started to test a spy tool able to register users navigation data, including pages visited and time spent in each one. This software has been developed by Phorm, a British company whose monitoring technologies have already raised controversy in several countries[25]. Oi, Velox controller, and Phorm have also announced an association with popular Brazilian Internet portals, including Terra, UOL and Estadão, which could target advertisements to their visitors based on information collected by the spy software.

Together, Oi and Telefonica provide 55% of broadband Internet access in the country. But as they act in different geographical areas, the Administrative Council of Economic Defense (CADE) approved Oi partnership with Phorm without restriction in October 2011. Telefonica partnership with Phorm was also approved two months later[26]. The Department of Consumer Protection and Defense, part of the Brazilian Ministry of Justice, has filed an administrative lawsuit against Oi in June 2010, to examine evidences of privacy intrusion. The company was invited to give some explanations about the software, but it did not respond. The lawsuit is still under analysis.

Currently, the most modern provision about data protection in Brazilian law is article 43 of the Consumer Defense Code, according to which people should be informed about their inclusion in databases and have open access to registered information about them [28]. The Complementary Law of Bank Secrecy (CL 105/201) and Habeas Data Law (9507/97) also contain legal provisions about data protection. Besides, the Brazilian Federal Constitution proclaims that "*privacy, private life, honor and image of people are inviolable*".

However, Brazil still does not have a dedicated personal data protection law. While in developed countries these laws started to emerge in the 1970s, only now legislators are discussing the matter in Brazil. The country is late even when compared to other Latin American nations: Chile consolidated a law about the issue in 1999, followed by Argentina, whose personal data protection law is the only one in the region in compliance with European rules. In 2010, Mexico also approved its Federal Law of Personal Data Protection.

Aiming to surpass this delay, the Ministry of Justice put a draft bill proposition before a public hearing in November 2010[27]. Inspired by the European Data Protection Law (95/46/EC), it aims to update citizens' rights about the current context of technological acceleration and progressive surveillance. It does not forbid data processing, admitting that, in some cases, it has a social value and can be useful to individuals. But it set the rules and conditions under which institutions can do it, and provides that people should not be submitted to decisions which heavily affect them, based only on an automated data processing. The proposition also gives people the right to ask institutions about techniques employed and patterns informing data processing. It also provides that they should consent and be notified of data collection in the very moment it takes place.

Other important draft bill proposition, also put before public hearing by the Ministry of Justice is the Internet Law Framework, which aims to define the technical structure and values that should guide Internet development in the country. It respects data protection directives and provides that people should be informed about how their data will be used. According to that, data processing, distribution and third parties access should depend on the users consent. This proposition has received more than two thousand contributions during the public hearing and it was presented to the National Congress in August 2011.

7. Privacy: Strength and Limitations

Taking the discussion above into account, is privacy a useful way to frame inquiries about data collection and usage as observed in Brazilian websites? Privacy is proclaimed to be a fundamental value for freedom and democracy [2][17]. On the other hand, some philosophers, sociologists and even legal scholars claim it is an inconsistent concept to face contemporary nuances of personal information flow [3]. The most common criticisms are directed towards the concept broadness and individualistic dimension[28].

One of the most prominent definitions of privacy is that of control over personal information. In Alan Westin's ([19], p. 7) words, "*privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent the information about them is communicated to others*". This concept of privacy, which has its roots in liberalism, is widely quoted as evidence of privacy as seclusion and individualism. As Steeves ([20], p. 11) says, Westin's analysis contains social aspects, but they fade as the focus of the author's argumentation shifts to the flow of information. Thus, privacy becomes antisocial and it is finally located in the individual's unilateral control against disclosure of his/her information.

As we have seen, the idea of individual control over personal information is recurrent in the online tracking discourse. Privacy policies and corporations claim that individuals can block cookies or opt-out while social actors and even legislators reinforce the importance of user notification and consent. But in practice, what we see is a context of pervasive and noiseless data collection, which cannot be faced only with individual informed choice, but one which depends on collective action[29]. Especially concerning Internet usage, conditions to autonomy cannot be centered on the subject, since they involve a network of technical, human, administrative, political, juridical and several other actors.

As we see it, the nature of this technology and the way it affects individuals should be a matter of public concern. It is eminently social, since it is the collective dimension of

> "Privacy policies and corporations claim that individuals can block cookies or opt-out while social actors and even legislators reinforce the importance of user notification and consent"

databases which permits, through statistical processing, the decision making process which is going to influence individual conduct. Furthermore, online tracking can be related to the emergence of potencial privacy problems with important social implications: threats to freedom of choice and discrimination; data usage to purposes unknown by the user; discrimination practices, with the denial of products and services to a specific group or individual and the leverage of price according to different profiles; boxing, which is defined as the limitation of the consumers' vision and choices by his/her digital history ([24], p. 673)[30].

In this sense, some questions can be raised: Is enhancing notice and respecting users consent all we need? Do we need to have the power of choice or specialists and regulators to answer these questions for us? Yes or no, opting in or out, does it define enough space for negotiating a value as important as privacy? We believe that the freedom of choice, control and notification play an important role in rescuing privacy, but we also need an adequate regulatory framework, able to reflect society's stand on the question.

8. Conclusion

HTTP cookies and web beacons are popular tracking mechanisms in Brazilian websites and the majority of them are set by companies in the online marketing field. Third party cookies are also widely used in the websites analyzed and tracking processes are obscure. Opt-out options are not always available and information about their reach is sometimes unclear and limited. This context is built in a legal and technological shell that is too complicated for common people to understand. Privacy policies are generic and apparently designed to place doubt and responsibility on the shoulders of the public, opening enormous possibilities for companies to collect, manage and use personal data. In addition, an adequate regulatory framework is still under development in the country.

Opt-out options and user choice are hard to exert given the lack of transparency of such a context. Moreover, they cannot be taken as an easy way to get rid of the obligation of giving an adequate political response to the privacy problems that arise by behavioral targeting practices. If current practices shrink the space for negotiation, it thus requires us to rescue the social value of privacy. Hence, it needs to be regulated and discussed in the field of collective action.

Acknowledgments

This investigation is part of a research project titled "The social effects of regulation and data processing in Latin America" (Forthcoming) that approaches three main fields: Internet, identification schemes and video surveillance. It has been carried out in two countries (Brazil and Mexico) and was funded by the International Development Research Centre – IDRC <http://www.idrc.ca/EN/Pages/default.aspx>.

References

[1] **O. Tene, J. Polonetsky.** *To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising*. August 31, 2011. <http://ssrn.com/abstract=1920505>.

[2] **D.J. Solove.** *Understanding Privacy*. Cambridge: Harvard University Press, 2008. ISBN: 0674027728.

[3] **F. Stalder.** Privacy is not the Antidote to Surveillance. *Surveillance and Society, 1 (1)*: 120-124, 2002.

[4] **B. Latour.** *Reassembling the Social*. Oxford: Oxford University Press, 2005.

[5] **T.Z. Zarsky.** Mine your own business! *Yale Journal of Law and Technology, 5 (1)*, 2002.

[6] **A. Soltani et al.** *Flash cookies and privacy*. August 10, 2009. <http://ssrn.com/abstract=1446862>. Accessed on May 12, 2011.

[7] **K. McKinley.** *Cleaning Up After Cookies*. Technical report, iSEC PARTNERS, 2008, <https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf>. Accessed on May 1, 2012.

[8] **C. Jackson, A. Bortz, D. Boneh, J. Mitchell.** Protecting Browser State from Web Privacy Attacks. *Proceedings of the 15th International Conference on World Wide Web*, May 23-26, 2006, Edinburgh, Scotland.

[9] **J. Angwin.** Latest in Web Tracking: Stealthy 'Supercookies'. *The Wall Street Journal, August 19, 2011*. <http://online.wsj.com/article/SB10001424053111903480904576508382675931492.html>. Accessed on April 29, 2012.

[10] **B. Krishnamurthy, C. Wills.** On the Leakage of Personally Identifiable Information Via Online Social Networks. *WOSN'09*, August 17, 2009, Barcelona, Spain.

[11] **Tanzina Vega.** Code That Tracks Users' Browsing Prompts Lawsuits. *The New York Times, September 20, 2010*. <http://www.nytimes.com/2010/09/21/technology/21cookie.html?_r=1&pagewanted=all>. Accessed on May 1, 2012.

[12] **A. Banks.** *State of the Internet in Brazil*. February 2011. <http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/State_of_the_Internet_in_Brazil>. Accessed on January 24, 2012.

[13] **CGI.br.** *Pesquisa TIC Domicílios 2010*. <http://www.cetic.br/usuarios/tic/2010/index.htm>. Accessed on February 11, 2012.

[14] **J. Valentino-Devries.** What they know about you. *The Wall Street Journal, July 31, 2010*. <http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html>. Accessed on January 20, 2012.

[15] **P.M. Schwartz, D.J. Solove.** The PII Problem. *NYU Law Review, 86 (6)*: pp. 1814-94, 2011.

[16] **D. Lyon.** *Surveillance as Social Sorting*. London and New York: Routledge, 2003. ISBN: 0415278724

[17] **C. Bennett.** In defence of privacy. *Surveillance & Society 8(4)*: pp. 485-496, 2011.

[18] **A. Miller.** *Assault on Privacy*. Ann Arbor: University of Michigan Press, 1971.

[19] **A. Westin.** *Privacy and Freedom*. Nueva York: Atheneum, 1970. ISBN: 0370013255.

[20] **V. Steeves.** Reclaiming the Social Value of Privacy. *Lessons from the Identity Trail, ed. I Kerr*. Oxford: Oxford University Press, 2008.

[21] **K. Purcell, J. Brenner, L. Rainie.** Targeted advertising: 59% of internet users have noticed it, but most don't like it. *Pew Internet & American Life Project, March 9, 2012*.

[22] **G. McMillan.** Less Than 1% of Firefox Users Use 'Do Not Track' Function. *Time Techland*, April 25, 2011. <http://techland.time.com/2011/04/25/less-than-1-of-firefox-users-use-do-not-track-function/>. Accessed on April 29, 2012.

[23] **A. Acquisti, L. John, G. Loewenstein.** What is privacy worth? *Twenty First Workshop on Information Systems and Economics* (WISE), Phoenix, Arizona, 2011.

[24] **M. Abrams.** Boxing and concepts of harm. *Privacy and Data Security Law Journal, September 2009*, pp. 673-676.

[25] **L. Scism, M. Maremont.** Test Data Profiles to Identify Risky Clients. *The Wall Street Journal*, November 18, 2010. <http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html?mod=wsj_share_twitter>. Accessed on May 1, 2012..

[26] **K. Hill.** How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. *Forbes*, February 12, 2012. <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>. Accessed on April 30, 2012.

[27] **S. Stevenson.** What your Klout score really means. *Epicenter*, April 24, 2012. <http://www.wired.com/epicenter/2012/04/ff_klout/all/1>. Accessed on April 30, 2012.

[28] **Idec, Instituto Brasileiro de Defesa do Consumidor.** Proteção de dados: Sorria, você está sendo monitorado. *Revista do Idec, n. 150*, December 2010.

Notes

[1] ***Cookies*** were created to cache applications state on users' computers and enhance their navigation performance, benefiting the user. On the one hand, they are useful as they make it possible for features such as saving passwords, retaining preferences (as volume or language) and files to be cached. But they can also be used to collect user's personal and Internet connection information (as an IP address and operational system details) and searches that users might have done in search engines. Since they are stored in the machines, giving it an identification number, they also enable

the tracking of pages visited thereon. HTTP cookies can be easily blocked through web browser's settings, but this can disturb the normal functioning of the website applications. Flash cookies are more resilient. They are not controlled by the browser. Thus, whatever you do in your browser (such as choosing private navigation options, erasing cache and so on) will not affect their functioning. In addition, Flash cookies are not stored in the same location as HTTP cookies, what makes it harder for the user to identify them [6]. Finally, web beacons are even harder to block because they are not files stored in web browsers. One example of this mechanism is the use of 1px transparent images, placed on a sequence of web pages, whose successive requests can be used to track user navigation.

[2] It can tell the kind of articles read, if you are in a news website, or can be collated with the product description bought, for example, enabling different profiles to emerge.

[3] It includes cookies as tracking methods that use browser information, client browser state or content cached in a web browser [7][8]. An example is "history stealing" tracking, in which a website checks if a user has visited other specific [9]. Other important source of information includes social network sites, that can be used to identify a user through its profile page on a certain social network [10].

[4] It enables agencies to manage the advertisements, their distribution and performance.

[5] When someone visits a website, the ad server delivers a cookie attached to the banner one sees. This cookie is stored on the user's computer, and when the person visits another website showing ads delivered by the same server, his/her browser sends the cookie back to the server. Thus, the person is identified and based on information that has been previously collected about his/her, the system can "decide" which ad to show.

[6] From the age of 15 and older, accessing Internet from home and work computers.

[7] Orkut <http://www.orkut.com> has led social network market in the country until December 2011, when Facebook <http://www.facebook.com> registered 36.1 million visitors and finally took over after a year of unprecedented growth.

[8] According to the ranking made by Alexa <http://www.alexa.com/topsites/countries/BR>. This ranking is ordered considering a combination of average daily visitors and pageviews over the past month.

[9] <http://www.terra.com.br/portal/>.

[10] <http://www.uol.com.br/>.

[11] <http://www.globo.com/>.

[12] <http://br.yahoo.com/>.

[13] <http://www.youtube.com/>.

[14] We have used Mozilla Firefox 4.0 and Windows XP Service Pack 2.

[15] <http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html>.

[16] <http://www.ghostery.com/>.

[17] For this analysis, we have chosen the most popular apps of five different categories. This measurement of popularity considers the application usage by social network community as a whole, not only used by Brazilians. The Orkut applications chosen were: Segredos do Mar, Buddy Poke, Colheita Feliz, Baby Adopter and Musica. On Facebook, we analyzed the following applications: Causes, Texas Hold'em, Phrases, Badoo and Quiz Planet.

[18] <http://www.robtex.com>.

[19] Cookie #1: Placed by a social network website platform developer or a non advertising partner of these developers; Cookie #2: Placed by a research company which produces general reports of internet use; Cookie #3: Social media websites cookie placed in third party websites; Cookie #4: Placed by a company which does not quote its name in the URL associated with the cookie; Cookie #5: Placed by a company which offers market targeting solutions or audience and interests measurement solutions for social apps developers and advertisement publishers; Cookie #6: Placed by a company which offers traffic and access measurement solutions, semantic content analysis solutions or mapping tools to understand user behavior, optimizing websites and apps; Cookie #7: Placed by the website owner or a non advertising partner of the website; Cookie #8: Cookie placed by a third party website which offers its service embedded in a specific section of the analyzed website.

[20] For social network websites, Flash cookies have not been examined.

[21] See note 19 for a description of the types of cookies. Beacon #1: Placed by a research company which produces general reports of internet use; Beacon #2: Social media websites beacon placed in third party websites; Beacon #3: Placed by a company which does not quote its name in the URL associated with the beacon; Beacon #4: Placed by a company which offers market targeting solutions or audience and interests measurement solutions for social apps developers and advertisement publishers; Beacon #5: Placed by a company which offers traffic and access measurement solutions, semantic content analysis solutions or mapping tools to understand user behavior, optimizing websites and apps; Beacon #6: Placed by the website owner or a non-advertising partner of the website.

[22] Network Advertising Initiative (NAI) <http://www.networkadvertising.org> is a coalition of online marketing companies involved with regulation and consumers education about online advertising. It also offers a centralized opt-out mechanism for some member companies.

[23] TRUSTe <http://www.truste.com> is a United States company which certificate websites according to its own privacy policies.

[24] Safe Harbor Privacy Principles is a process that the United States corporations use to indicate comply with European Union Data Protection Directive - EU Directive 95/46/EC.

[25] In 2009, the service, tested in the United Kingdom by British Telecom, was considered illegal by the European Commission.

[26] The lawsuits 08012.010585/2010-29 and 08012.003107/2010-62 are available at <http://www.cade.gov.br/Default.aspx>.

[27] The public debate is available at <http://culturadigital.br/dadospessoais>. The period for public hearing ended in March 2010. By now, the bill have not been sent to the National Congress.

[28] Miller [18, p. 25) says "*privacy is difficult to define because it is exasperatingly vague and evanescent*". Stalder [3, p. 3) claims that the "*bubble theory of privacy – based on concepts of individualism and separation –* (…) *applies a 19th century conceptual framework to a 21st century problem*". Lyon ([16] considers the concept is insufficient to face discrimination conditions prompted by social sorting: "*surveillance is not merely a matter of personal privacy but of social justice*".

[29] This approach is partly based in recent studies which show that user's practices and discourse towards privacy are ambiguous. On the one hand, users claim to be uncomfortable with behavioral advertising [21], but on the other hand, they usually do not take any attitude, no matter how effortless, to prevent their data from being collected [22]. Added to this, they seem to be likely to give away personal data even for small rewards [23]. It claims for a discussion that considers the value of online tracking not only to individuals, but also to broader society.

[30] Even though an adequate comprehension of these implications (or privacy problems) would require a deeper investigation – what would surpass the objectives of this preliminary study – harmful consequences of profiling practices are shown in the literature and newspaper articles. For instance, British insurer Aviva has been using market data to estimates people's risk for illnesses related to their lifestyles, raising concerns about denial of applicants and the leverage of price according to the consumer profile [25]. Target, a US-based retail chain, has been using purchase information to predict pregnancy, what ended up revealing to a father the pregnancy of his teenage daughter [26]. Sam Fiorella has been overlooked for a job despite her 15 years of experience because of her Klout.com score, a service that measures user's online influence without they even know about its existence, based on public information of social media accounts [27].

Massimo Ragnedda
University of Northumbria, Newcastle (United Kingdom)

<ragnedda@gmail.com>

Social Networks and the Protection of Personal Information. When Privacy Is Not Perceived As a Right

Abstract: *On Social Networking Sites (SNS), users freely and without anxiety give sensitive and private data about which they might previously have jealously guarded. The research that I conducted at the University of Sassari (n = 1047), suggests that students have a different approach to the protection of Personal Information: lascivious online and protectionist offline. Students seem to underestimate the risk of posting data because they are unaware of the phenomenon of dataveillance. In fact, 86% said that the main visitors of their personal profile are friends, so they do not worry about data because they have nothing to hide from friends. This makes the perception of SNS more familiar and intimate and lowers social and cultural defenses against the possible intrusion of strangers in their digital world. Only 29.4% said that they often or always heed the privacy policy before registering for a site, and 54% never or rarely read the privacy policy. The role of marketing agencies that scan, match and connect data of individual users with the goal of building an accurate e-profile profile of individual users, seems not be perceived by the students. In fact only 3% imagine that those who visit personal profiles are strangers.*

Keywords: *Dataveillance, e-Profile, Privacy, Social Networking Sites, Surveillance.*

Author

Massimo Ragnedda is a Ph.D. in Theory of Communication and Intercultural Studies at the University of Sassari (Italy). In the academic year 2003/2004 he was a Visiting Researcher at the Institute of Communication Studies of Leeds University (UK), in the academic year 2006/2007 he was an affiliated visitor at the Department of Sociology, University of Cambridge (UK) and he was Academic Visiting at the Oxford Internet Institute (University of Oxford). Currently he teaches Mass Communications at Northumbria University (UK). He is author of 6 books and several articles in Italian, English and Spanish.

1. Introduction

The last decade has been characterized by the enormous development of Social Networking Sites (SNS), able to offer a range of new opportunities for communication and exchange of information of any kind, in real time, unimaginable until recently [1].

The incredible success of sites like Facebook reveals a radical change in the public accessibility of personal data of users. Facebook users extend their social circle and share data and information with their community and their friends, regardless that such information is distributed through third parties who collect them and gather in large databases [2]. Users produce content and add data by clicking the "Like" button on the content of others, regardless it comes from a friend or from external websites. Those "Like" clicks help to enrich the map of relationships (social graph) with multiple demographics that then help in locating the most suitable target for advertisements.

Using the SNS raises, therefore, a whole set of questions about the possible risks that their use leads to violation of privacy [3a][3b][3c]. Users of social networks do not always perceive the risk to their privacy [4]. The network is, in fact, an irreplaceable instrument of collective memory, capable of reflecting and building digital identities of users that are present online. Privacy becomes, thus, a key element for the construction of personal identities [5a][5b].

These dynamics, typical of the digital age, introduce profound and irreversible changes in our way of living and relating. With the advent of SNS it is changed, for a relevant part of the population, the way they relate to others, some fundamental principles of social life, and the conception and perception of privacy.

The Internet users in general and the users of the SNS in particular, tend to give freely, and without hesitation, the personal data about which they were once zealously guarded. But free does not mean, however, "at no cost": in fact, many SNS reuse the data entered into the personal profiles and sell them for marketing activities [6].

The act of sharing photos, political or religious views, sexual orientation and other private data, gives the possibility to create an increasingly defined electronic profile. The growing need for finance services and benefits is a stimulus for the collection, processing and use of user data. In fact, the information in "private" profiles is the only real heritage asset managers of SNS have, so the risk that these data are picked up, analysed and used, is increasing [7].

The hypothesis we propose here is that the right to privacy seems to be perceived, especially by Internet users as a right that is becoming less important and less valued. However, we are talking about a vitally important right in a democracy, because the protection of personal data guarantees the individual freedom [8]. Having the right to privacy means preserving social capital created in private, invested in relationships and friendships, and the lack of which can compromise social relations [9]. The right to privacy is a value [10] that must be defended [11] as an intrinsic value for the society [12]. Although the concept of "privacy" is imprecise [13a][13b], Turn stressed [14] that it should be considered as the right of individuals to the collection, processing, dissemination and use of their personal information.

At the same level as public monitoring, also the large corporations use surveillance for private purposes [15]. Private companies are interested in developing consumer profiles, and to build it, day after day, they use personal data which users type in the SNS and that are publicly (and globally) accessible in unknown terms and quantities. Peter Von Zschunke, for example, has been identified in a sample of the most popular SNS, about 120 personal attributes in user profiles: an impressive amount of personal data available with a mouse click [16].

The idea of controlling and gaining the maximum amount of data on citizens is not new. In fact, and as stressed by David Lyon, the creation of personnel files and the need to collect information on individuals gradually extended from military fields to all sectors of public and civil life, to become one of the elements that characterize the modern state [17].

Modernity is based in the process of bureaucratization and rationalization which Weber described, and that has characterized the historical process, also in the collection of data and information about individual users. This collection of information has become something that is increasingly present and yet invisible, which serves the principles of the

> "What sets this current model is the incredible amount of information that can be collected today from citizens and the relationship that individuals have with their own personal data"

Panopticon, the model prison that was first developed in 1791 by Jeremy Bentham and adopted by Foucault as a metaphor to describe and explain the operation of discipline and surveillance of individuals throughout the modern era.

What sets this current model is the incredible amount of information that can be collected today from citizens and the relationship that individuals have with their own personal data.

We all become the subject of attention. We live in a kind of cyberpanopticon [18], or superpanopticon [19], in an electronic surveillance system [20], in which the jailer's eyes constantly watch us. As in the panopticon, where the watchful eye is unverifiable, but always potentially present, the ability to record and reconstruct the individual profile of each individual "navigator" allows the Internet to go a step further than the Bentham project. The centre controls the periphery, which is controlled from the top down, but also reconstructs the individual's profile, linking a set of data and images for each individual user.

Based on these assumptions I have developed a research that aims to find out how the "digital natives" [21] perceive the risks of losing privacy while using social networking sites.

Specifically, the question that has guided this research project, conducted with students of the University of Sassari (Italy), that it will be discussed in this article is: How is our relationship to privacy changing? And on this question: Do we act differently in online and offline environments? What are the risks facing this difference to privacy?

2. Methodology

Sassari University has over 15,000 students divided into 11 different faculties [22]. We contacted participants through the mailing list of the Secretariat of Students, who sent the questionnaire via e-mail to all students of the University of Sassari. The questionnaire was tested on a sample of 15 students and was available online (after some modifications), for two months, from 14 September to 12 November 2011.

1,068 students responded, but 21 questionnaires were incomplete or were totally incomprehensible and were discarded. The 1,047 valid questionnaires constituted a representative sample of the University of Sassari. The most active Faculty was the Faculty of Literature (belonging to Area Social and Humanistic), with 38%, followed by the area of Law and Political Science with 23.7%, and the physical and medical sciences to 20.8 %. There were a greater participation of women (54.5%) than men (45.5%).

The questionnaire includes 40 questions and is divided into four sections: the first on registry data, a section on the online habits of students, a very specific perception of privacy and surveillance, and finally, a section focused on the relationship between social and political networks. The results have been elaborated with SPSS 18.0 for Windows.

3. Main Results

In the context of this research, what stands out is the absolute confidence that students have with the Internet as the medium that has revolutionized the way they express themselves and that helps them to enter into the labour market: in fact, 46.9% say that the Internet has increased their chances of finding jobs, as well as has increased the opportunity to be found on the network on which they have, or should have, an appropriate profile that gives a good impression of themselves.

In fact, according to research cited by the Guarantor for the Protection of Personal Data, the administrative authority which protects access to user data in Italy, 77% of recruiting staff check on Internet seeking potential candidates and 35% say have eliminated candidates based on information discovered in the network.

Caring for one's image and reputation online is becoming very important as more and more companies in the pursuit of personal support or reject candidates thanks to the information that can be found on the network.

In order to understand the perception that students have of this phenomenon, I have asked the following question: "*Will entrepreneurs increase the use of Facebook to manage their current and potential employees?*". 58.6% of the sample agree or absolutely agree with this statement, and only 19.3% said they disagree or strongly disagree. Most respondents have, therefore, the perception that Facebook, and the vast amount of personal data it contains, could be used to select or monitor employees.

However and here it comes the first contradictory data: Indeed only 37.8% of the sample believes that the profile gives an accurate picture of them. In other words, despite being aware that potential employers can use Facebook to select or control their workers, most of the students seem not to worry about how they build them online profile and how accurate is. In fact, only 0.3% (ie, only 3 people in 1,047), believes that those who visit their profile is a possible recruiter.

Slightly better is the fact that references to (the future, that is), who will be the main visitor in the future: only 2.2% of the responded said the potential recruiters. A very low percentage comes out even for cases in which we talk about the potential of state surveillance. In fact, only 0.7% believes the government visits their profile and only 3.7% think that it will do so in the future.

These data demonstrate that students underestimate the long memory of the network and how data can be purchased by individuals who are not part of their group of friends, that 86.3% are the main visitors of the profile.

Probably the term "community" confuses the point of view and makes us believe that the data is shared "only" with the reference community. Actually, you never know for sure who is the public with whom data are shared, unlike offline life, where it is well known to those who hear our conversations, who are watching us and those around us. While we are online we do not know who is on the other side recording or collecting information.

From the data obtained by the research, there emerges a main difference in the management of privacy online and offline. Indeed, the research shows that students, overall, are very attentive to their offline privacy, to act accordingly, and they have an absolute protection of personal data.

We cannot say the same for their online activities. In particular, 37.9% of students who responded to the questionnaire said they always destroy their private documents when no longer useful, to which must be added 19.1% who do it sometimes. More than half of respondents, 57.0% destroy often or sometimes, forever and without proper backup, personal documents. Only 22.4% said no and 20.6% rarely do (see **Figure 1**).

This denotes a personal data protection which is very high, precisely to prevent others from accessing them. On the Internet, however, they neglect the possibility that the data can be forgotten or destroyed. Once published, and

> “These data demonstrate that students underestimate the long memory of the network and how data can be purchased by individuals who are not part of their group of friends”

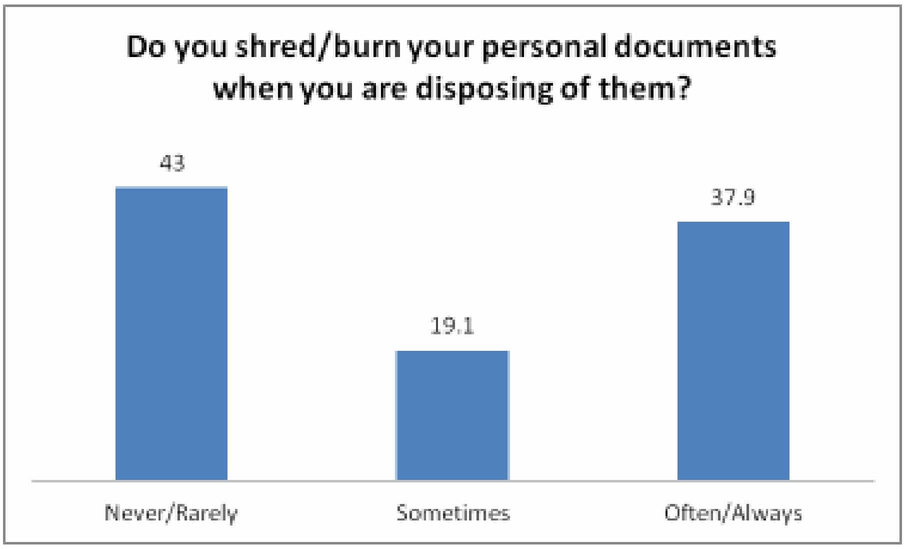


Figure 1. Do you shred/burn your personal documents when you are disposing of them?

even if they are deleted from the page in which they were originally inserted, there is no certainty that these data finally disappear.

Returning to the offline sphere, 80.8% say they protect or hide, usually or always PIN credit card when they use it. This means that 4 out of 5 people protect this important data. Only one in 20 (5.3%), never fail to protect their PIN (see **Figure 2**). Most respondents show prudent behaviour in this regard.

We cannot say the same, although this is not as important as data PIN credit card, the behaviour of these same students in managing their data online. For example, only 34.9% of students are registered, usually or always, exclusively on websites that have a privacy policies, while 39.7% never do or do so rarely, and 25.4% do so sometimes. (see **Figure 3**).

There is more. Only 25.9% said they always or sometimes read the privacy policy if present. In fact, 54.0% never read, or rarely read the rules that protect their own right to privacy, and 20.1% do it once (see **Figure 4**).

In other words, more than half of the sample gives personal information without knowing how that data will be used, and this reflects the idea that they are not interested in managing and protecting personal data. To this we should add that one in four people always read the policy. It seems that the right to privacy does not interest them so much, that the perception of privacy as a right is disappearing, and they do not pay attention to the consequences that could result from the publication of personal data in a private profile that is only partly private.

Using a pseudonym to register on a website, without having to reveal the true identity to the other service users or the general public, can help to manage personal data. Only a quarter of respondents, 24.6% stated that never or almost never complete certain information when registering on a SNS. More than half of the sample, 51.6% always or often does, and the remainder, 23.7%, sometimes does.

Among the most regularly published data on SNS users, we can find the real name (84%), followed by the date of birth (81.5%), favourite links (74.9%) and favourite music bands (73.3%). On the other side, the data published in the SNS less published are: embarrassing photos of themselves (88.9%), telephone number (87.8%) and home address (87%). An interesting aspect to underline is that only 37.9% post their curriculum online, although it may be one way to get noticed.

Not only in the SNS we leave traces about ourselves: every move on the net leaves a trail behind it, a small sign but a really important sign for those who want to rebuild our profile and understand our tastes and preferences. As experts of the Electronic Privacy Information Centre underlined it is important to delete cookies [23] and clean regularly the visiting history, precisely because this gesture makes it more difficult to collect data from our online tour. Only 40.8% of the students interviewed stated that always or often they delete cookies. This finding is particularly significant because college students have, at least it should have, better computer skills than the rest of the population, and therefore we can assume that this data should be significantly higher than the rest part of population. The same statement we can assume about the habit to regularly clean visiting history: 43.1% say they rarely or never do it.

Managing and protecting personal data also involves respecting the privacy of others, especially when publishing personal data or photographs without permission. In this study we

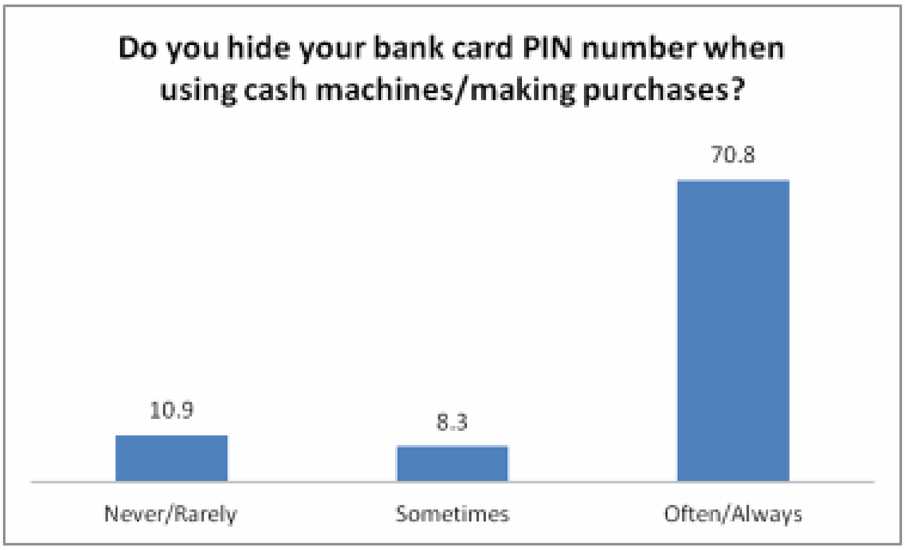


Figure 2. Do you hide your bank card PIN number when using cash machines/making purchases?

> “Not only in the Social Networking Sites (SNS) we leave traces about ourselves: every move on the net leaves a trail behind it”

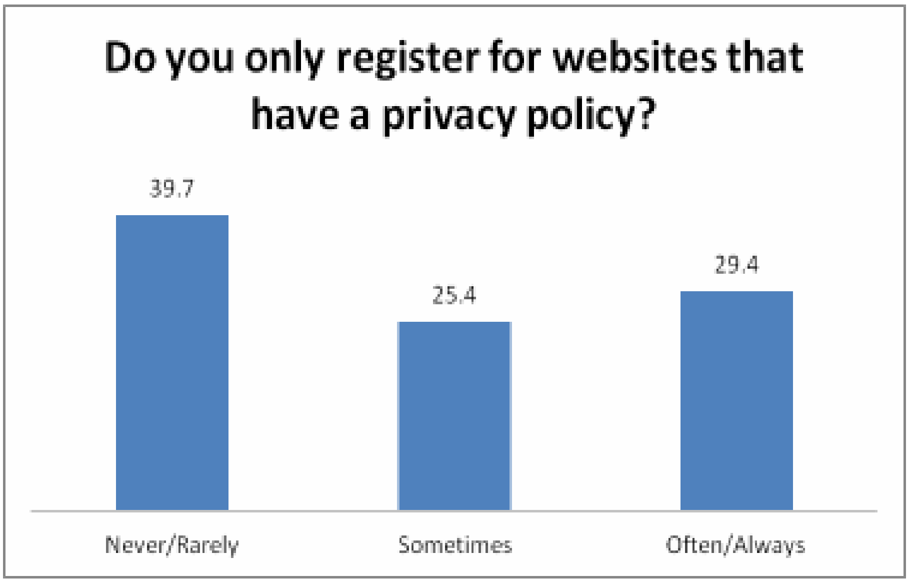


Figure 3. Do you only register for websites that have a privacy policy?

found that only 42.2% of the students always or almost always ask permission to others before posting a photo or video in which they appear. The risks are significant. Photos can, for example, thanks to the increasingly sophisticated technologies and through facial recognition software, turn into biometric identifiers. All these aspects can compromise the privacy and security of other users. And despite this, 37.1% of the sample, more than one person out of three, says that never ask permission to publish photographs or videos of others.

The practice of publishing news and personal information on others, although not usual, is present. In fact, 19.5% of respondents said that they sometimes publish information about others, and 6.6% do so often. Thus published information can damage privacy.

4. Notes for Reflection and Conclusion

The SNS questions the concept of "personal space" in its social meaning and personal and private data becoming public data through initiative coming from the users. To be more precise, as Royer, Deuker and Rannenberg say [23], the concept of privacy is moved from a static that affects only the privacy, to a dynamic process control limit that operates between subject and that which surrounds it. This significantly complicates the legislation of privacy protection. So far the privacy legislation protects the right to live in peace and from unfair treatment of personal data. Now, however, is the same user who voluntarily gives up their data, and there are few rules governing the publication of personal data in the context in which this transfer occurs with the consent of the citizens.

In this regard, two issues stand out clearly: the digital natives, born and raised in a computerized environment, are less aware of the risk to their privacy than those who come as adults to the world of Internet. The second point to be drawn from all this is that the same person is more careful of his/her privacy offline than online. In the network the citizen has less concerns to make public personal information. And yet, the online and offline worlds interpenetrate and interact with each other with continuous references.

Students underestimate the danger of privacy violation and the transfer of personal data because no attention is paid to the phenomenon of surveillance data-network [24]. The fact that the vast majority declare that the main visitors of their profile are their friends underline that they are not too worried about hiding information, so they do not worry about data because they have nothing to hide from friends. This makes the social network perceived as an instrument familiar and intimate and the cultural defences against the possible intrusion of strangers into their world, tends to decrease.

In this study, the students completely underestimate the role of marketing agencies that collect, analyse and link user data to build an online profile as faithful as possible. Less than one student in three noted that they always or almost always read the privacy policy before registering on a website. Two people out of three don’t show any interest in how their personal data will be treated and in the rules to manage their right to privacy.

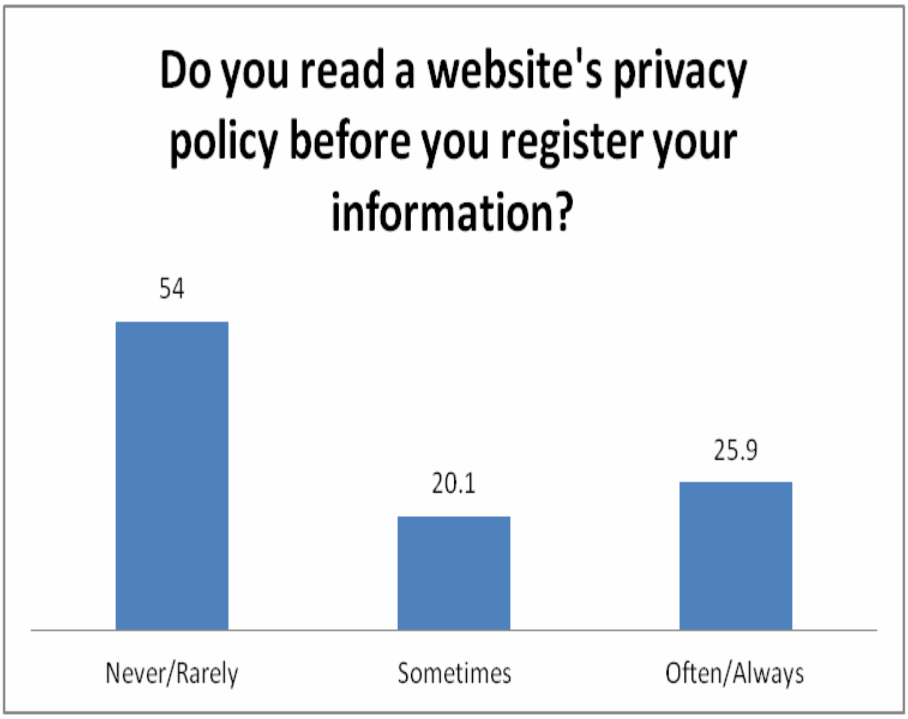


Figure 4. Do you read a website’s privacy policy before you register your information?

> “Two people out of three don’t show any interest in how their personal data will be treated and in the rules to manage their right to privacy”

This research also reveals that there are two different ways of managing and protecting the privacy: lewd online and worried offline, as if the two worlds were far away, as if the data collected online were not useful for the surveillance system, that is more and more inclusive, and for the construction of an e-profile constantly informed by the citizens and the consumers. The new surveillance system keeps under observation, not only the people at potential risk, but all those who in some way release, voluntarily or not, personal data in the network.

Regardless of what this violation of privacy is, we are running the risk of turning our private lives in a "continuous public life" [25]. It is losing the separation between public life and private life, we are becoming vulnerable and we risk losing an important capital that gives value and importance to ourself and our relationships. The information we create and we give for free makes us controllable. It is the loss of the right to privacy that makes us more vulnerable and it makes difficult to build trust between individuals [26].

References

[1] **D.M. Boyd, N.B. Ellison.** "Social network sites: Definition, history, and scholarship". *Journal of Computer-Mediated Communication*, 13(1), 2007. Article 11, <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html> (Feb 27, 2012).

[2] **R. Gross, A. Acquisti.** "Information revelation and privacy in online social networks". *Proceedings of WPES’05* (pp. 71-80). Alexandria, VA: ACM, 2005, <http://rio.ecs.umass.edu/~lgao/ece697_10/Paper/privacy.pdf> (Feb 27, 2012).

[3a] **S. Barnes.** "A privacy paradox: Social networking in the United States", *First Monday*, V.11, N.9-4 Sept. 2006, <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312> (Feb 27, 2012).

[3b] **F. Stutzman.** "An Evaluation of Identity-Sharing Behavior in Social Network Communities". *International Digital and Media Arts Journal*, 3(1), pp. 10-18.

[3c] **M.J. Hodge.** "Comment: The Fourth Amendment and Privacy Issues on the ‘New’ Internet. Facebook.com and Myspace.com." *Southern Illinois University Law School Journal*, 2006, 31, pp. 95–122.

[4] **A. Ho, A. Maiga, E. Aimeur.** "Privacy protection issues in social networking sites". *Computer Systems and Applications*, Seventh ACS/IEEE International Conference, pp. 271-278, 2009.

[5a] **W.S. Brown.** "Ontological Security, Existential Anxiety and Work place Privacy". *Journal of Business Ethics 23*: pp. 61–65, 2000.

[5b] **D. Nye.** "The ‘privacy in employment’ critique: a consideration of some of the arguments for ‘ethical’ HRM professional practice". *Business Ethics: A European Review* (11:3): pp. 224–232, 2002.

[6] **C. Fuchs.** "Web 2.0, prosumption, and surveillance". *Surveillance & Society* 8 (3): pp. 288-309, 2011.

[7] **J. Lawford.** "Confidence, privacy and security". *OECD-Canada Technology Foresight Forum*, Session 4b, 2007, <http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf>. (Feb 27, 2012).

[8] **P. Brey.** "Disclosive Computer Ethics". En R.A. Spinello, H.T. Tavani (eds.): *Readings in Cyberethics*. Sudbury, Massachusetts et al.: Jones and Bartlett: pp. 51–62, 2001.

[9] **L. Introna.** "Privacy and the Computer - Why We Need Privacy in the Information Society". En R.M. Baird, R.R. Ramsower, S.E. Rosenbaum (eds.): *Cyberethics - Social and Moral Issues in the Computer Age*. New York: Prometheus Books: pp. 188–199, 2000.

[10] **J. Rachels.** "Why is Privacy Important," *Philosophy and Public Affairs,* vol. 4, 4, 1975.

[11] **R. Spinello.** *Cyberethics: Morality and Law in Cyberspace*. London: Jones and Bartlett, 2000.

[12] **H. Tavani.** "Privacy and Security". En D. Langford (ed.): *Internet Ethics*. London: McMillan: pp. 65–89, 2000.

[13a] **D. Solove.** *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

[13b] **F. Stalder.** "Opinion. Privacy is not the antidote to surveillance". *Surveillance & Society* 1 (1): pp. 120-124, 2002.

[14] **R. Turn.** "Privacy Protection in Information Systems". En M.C. Yovits (ed.) *Advances in Computers*, 1977, p. 242.

[15] **M. Ragnedda.** "Social control and surveillance in the society of consumers". *International Journal of Sociology and Anthropology* Vol. 3(6), pp. 180–188, June 2011, <http://www.academicjournals.org/ijsa/PDF/pdf2011/June/Regnedda.pdf> (Feb 27, 2012).

[16] **V.P. Zschunke.** "*Mehr Informationen als die Stasi. Millionen von Internetnutzern drängen in soziale Netzwerke wie StudiVZ und Facebook*", *Berliner Morgenpost*, 23th January 2008, p. 9. <http://www.morgenpost.de/printarchiv/wissen/article160543/Mehr_Informationen_als_die_Stasi.html> (Feb 27, 2012).

[17] **D. Lyon.** *L’occhio elettronico. Privacy e filosofia della sorveglianza*, Feltrinelli, Milano, 1997.

[18] **G. Bousquet.** "Space, Power, Globalization: The Internet Symptom". *Societies*, 4: pp. 105-113, 1998,

[19] **M. Poster.** *The mode of information: Poststructuralism and social context*. Chicago: University of Chicago Press, 1990.

[20] **D. Lyon.** *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London–New York: Routledge, 2002.

[21] **U. Gasser, J. Palfrey.** *Born Digital - Connecting with a Global Generation of Digital Natives*. Perseus Publishing, 2008.

[22] **epic.org.** *Online Guide to Practical Privacy Tools*, <http://epic.org/privacy/tools.html> (Feb 27, 2012).

[23] **D. Royer. A. Deuker, K. Rannenberg (Eds.).** *The Future of Identity - Challenges and Opportunities*. Springer, Heidelberg, Germany, 2009.

[24] **R. Clarke.** "*Introduction to Dataveillance and Information Privacy, and Definitions of Terms*", 15th August 1997, <http://www.rogerclarke.com/DV/Intro.html>.

[25] **S. Rodotà.** *Intervista su privacy e libertà*, Laterza, Roma-Bari, 2005.

[26] **D.G. Johnson.** *Computer Ethics*. 3rd edition Upper Saddle River, New Jersey: Prentice Hall, 2001.

Joan Figueras Tugas
Systems and Information Technology Manager at Brosa Abogados y Economistas, S.L.P.

<joanfi@atinet.es>

Privacy and Body Scanners at EU Airports

Abstract: *At the beginning of 2010, with the aim of improving aviation security controls, some airports started to use full-body security scanners, also known as body scanners or security scanners. Body scanners make a full body screening of passengers, producing detailed images of the screened person's body in order to detect both metallic and non metallic objects that might be concealed under the clothes. Deployment of such scanners may entail an invasion of people's privacy since they produce a detailed display of the passenger's body with no clothing, revealing anatomical details and private parts, including medical prostheses. This article will analyse the currently existing screening technologies (millimetre wave systems -active or passive- and X-ray backscatter systems) as well as their level of deployment at EU airports, focusing on the impact they may have on passengers' privacy. In order to harmonize the various national regulations, the European Commission has passed a proposal on the use of body scanners at European airports, scanners which shall only be used under specific conditions.*

Keywords: *Access Control, Airports, Body Scanners, Privacy, Security, Security Scanners.*

Author

Joan Figueras Tugas holds a BSc in Electronic Engineering and a Master's Degree in Information and Communication Systems Management. He has focused his professional career on computing consultancy services, specializing in information security. He is currently the IT & Security Manager at *Brosa Abogados y Economistas*. He also renders professional advice to the clients of the Firm on privacy, data protection and information security. He is a member of the Spanish Association of Computer Technicians (ATI), the Spanish Association of Privacy Professionals (APEP), the Association for the Development of Information Security (ISMS Forum), and ISACA.

1. Introduction

On Christmas day 2009, Northwest Airlines flight 253 from Amsterdam to Detroit suffered an attempted terrorist attack when a passenger tried to detonate an explosive artefact during the flight. The author of the attempted terrorist attack had managed to board the plane with liquid explosives concealed in his underwear, which were not detected by the security controls at the airport. This incident made authorities in charge of security across the various European States give the green light to deploy body scanners at their airports.

Body scanners are able to detect both metallic and non-metallic objects, including plastics and liquid explosives, concealed under passengers' clothing. This article will analyse the different types of body scanners deployed to date, all having in common the capability to display a graphic image of the screened person's body.

Treatment of images produced by the scanners does have a great impact on privacy and human dignity, directly affecting certain fundamental rights laid down in the Universal Declaration of Human Rights and in the Charter of Fundamental Rights of the European Union.

Taking into account the definition of personal data laid down in article 2(a) of Directive 95/46/EC of the European Parliament and of the Council as *"any information relating to an identified or identifiable natural person"*, where the "physiological identity" is considered, among others, as an identifying item, there is no doubt that the body images produced by a body scanner are personal data and, therefore, their treatment must fully comply with all the guarantees of respect to the rights and obligations set out by the Directive.

In addition to protection of personal data, privacy and other fundamental rights (human dignity, freedom of movement, physical integrity or non-discrimination) are at stake. Are we willing to give up privacy in favour of greater security? In the aftermath of the attempted terrorist attack on Christmas day 2009, some European countries deployed security scanners, previously in trial. Then, after nearly two years, in which time each country set its own rules, the European Commission adopted in November 2011 a proposal for a legal framework on the use of security scanners. In this context, we will tackle the impact of this regulation on users' privacy.

1.1. Methodology

This article tackles three aspects in regard with body scanners: a) technical and operational equipment issues; b) European Union legal framework; and c) level of deployment of scanners at EU airports. Information to write this article has been directly obtained from the involved entities (manufacturers, institutions and aviation operators respectively).

Aside from the publications stated in the section "References", information provided by the manufacturers through their corporate websites has been taken into consideration in order to analyse the different technologies. The companies consulted have been (in alphabetical order): *Alfa Imaging*, *American Science and Engineering Inc* (AS&E), *Brijot Imaging System*, *EMIT Technologies*, *Farran Technologies*, *L3 Communications*, *Millivision Technologies*, *Rapiscan Systems*, *Smiths Detection*.

So as to have an insight into the current situation at EU airports, a brief questionnaire was sent to the aviation operators of the countries which had started to conduct body scanner trials, states which are listed on the "Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners", comments on which will be made further on. The questionnaire was sent in February 2012 and all the consulted operators responded. The questionnaire posed four open-ended questions:
a) Have body scanners been installed at the airport of…?
b) If they have, are they operating on an experimental basis or are they operating as an additional security measure of access control?
c) If they have not, is installation of such devices being planned, even on an experimental basis?
d) If these scanners are being used or their use is being planned, will passengers be forced to go through the scanners, or will they be allowed to opt for alternative methods such as "pat down"?

The bodies consulted have been: Aéroports de Paris (ADP) (France), AENA (Spain), Department for Transport - Aviation Security (UK), Direction Générale de l'Aviation Civile (DGAC) (France), Ente Nazionale dell'Aviazione Civile (ENAC) (Italy), Finavia Corporation (Finland), Fraport AG (Germany), Københavns Lufthavne A/S (Den-

> “ Treatment of images produced by the scanners does have a great impact on privacy and human dignity, directly affecting certain fundamental rights laid down in the Universal Declaration of Human Rights and in the Charter of Fundamental Rights of the European Union ”

mark), Schiphol Nederland B.V. (Netherlands). The information received has been complemented and contrasted with the information available in the analysed airport websites.

2. Body Scanner Technologies

Body scanners are person screening devices based on Advanced Imaging Technologies (AIT).

These technologies are able to reveal a display of a person's naked body, detecting objects that might be concealed underneath a person's clothing. Users must step inside an arch or portal (or stand in front of it, depending on the type of device) and stand still for several seconds while a scan of the full body takes place by means of electromagnetic waves. These waves pass through the clothing and reflect off the person's skin, allowing the AIT software to produce a body image of the individual.

Various types of body scanners are commercially available for security controls in the aviation sector. According to the electromagnetic wave frequency used, we can classify scanners in three groups: **X-ray**, **millimetre-wave** and **sub-millimetre-wave** (see **Table 1**).

We analyse below some of the technical and operating aspects of each of these scanners. Whereas in the USA, X-ray scanners (backscatter type*)* have been widely deployed, in Europe tests have been conducted with backscatter and millimetre-wave scanners. However, from November 2011 the European Commission has expressly prohibited the deployment of X-ray scanners, allowing the use of any other technologies.

2.1. X-ray

There are two ways to obtain an image by exposure to X-rays: *Transmitted X-ray* and *Backscatter X-ray* [1].

Transmitted X-ray emits X-rays like medical X-ray equipment, that penetrate the body and are capable of detecting concealed objects inserted into the body. Although this type of screening can be used under exceptional conditions, they are not used in security scanners since they produce ionising radiations which can cause adverse health effects.

Backscatter X-ray scanners emit low doses of electromagnetic X-ray waves which are able to pass through the clothing although they are reflected off the human skin and will not penetrate it.

A high resolution two-dimensional image is formed from capture of the reflected photons, the image revealing some surface detail of the body of the screened person, as if it were naked. If an object, metallic or non-metallic, were underneath the clothing, it would be revealed in the scanned image.

AS&E and *Rapiscan Systems* provide this type of scanners in the market. The UK Department for Transport (DfT), after trialling *Rapiscan Backscatter 1000* scanners, published a report [2] in February 2010 on the risks to health from exposure to this equipment. The experts concluded that the radiation dose from one scan was 0.02 micro Sierverts (ìSv), a small fraction of the maximum annual recommended radiation (2,700 ìSv). In comparison, the typical dose rate during a commercial flight from cosmic rays is approximately 5 ìSv/h.

2.2. Millimetre-Wave Scanner MMW

Millimetre-wave scanners use the Extremely High Frequency (EHF) radio frequency band, operating in the range 30 to 300 GHz. Within this range of frequencies, the waves pass easily through textile fabrics but cannot penetrate human skin. In addition, part of the thermal radiation emitted by the human body is within this range of frequencies, which therefore allows carrying out both passive and active scans.

Passive millimetre Wave *(Passive MMW)* **scanners** register the natural thermal radiation which is emitted by the body and produces images in contrast to the thermal radiation emitted by the environment. Good results are obtained with this technology in outdoor applications where thermal radiation contrast is significant. However, when it is operated inside buildings (such as in airports), it produces low resolution images and little reliability [3] due to a poor signal to noise ratio (SNR).

Brijot Imaging System, *Millivision Technologies*, and *Alfa Imaging* have developed equipment with passive MMW for airport control (see **Figure 1**[1]).

Active millimetre Wave (*Active MMW*) **scanners** generate EHF radiations which

Radio wave	Type of scanner	Name	Frequency	Wave-length
X-ray	Transmission	Transmission	30 - 3.000 PHz	10 - 0.01 nm
	Backscatter	Backscatter		
Millimetre-wave (MMW)	Passive	Passive MMW	30 - 300 GHz	10 - 1 mm
	Active	Active MMW		
Sub-millimetre wave (SMW or THz)	Passive	Passive SMW	0.3 - 3 THz	1 - 0.1 mm
	Active	Active SMW		

Table 1. Classification of Body Scanners According to Operating Frequencies.

> “… The communication, aiming at establishing a harmonised common framework on the use of scanners, deals with technical equipment issues, passengers´ health protection and users’ fundamental data rights ”

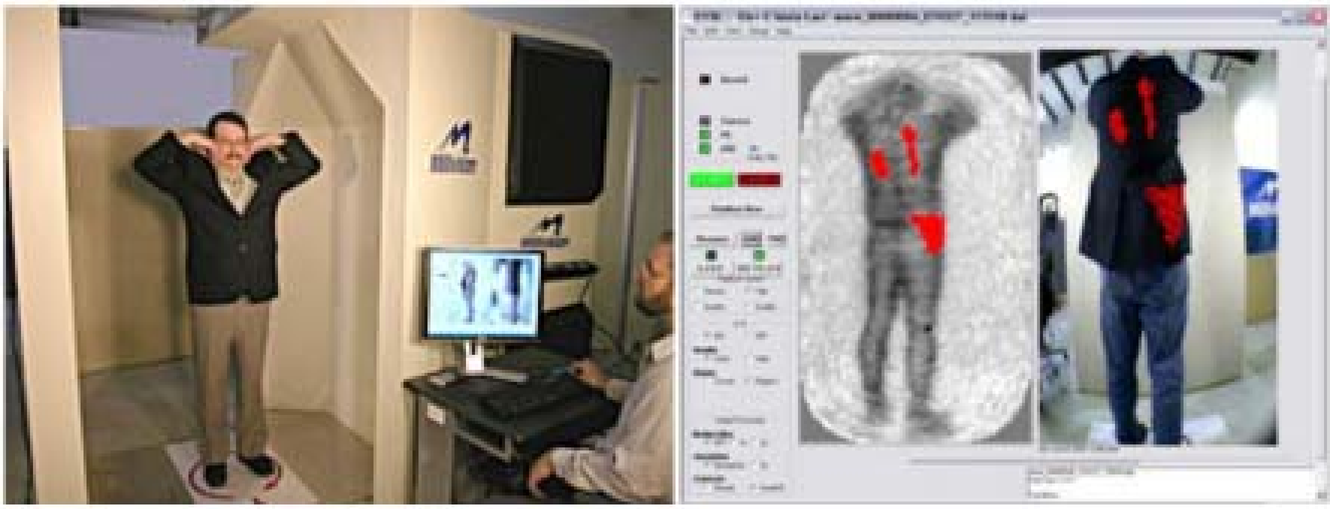


Figure 1. Millivision Portal Systems 350 scanner. On the Right, Screen Display Where ATD Software Enhances Threat. items.

pass through passengers’ clothing and reflect off the human body. From the reflected waves a three-dimensional image is obtained of the human body and of any objects being worn. This results in a detailed anatomical and high resolution image.

L3 Communications provides various active MMW in the market, some of them using ATD (*Automated Target Detection*) technology with which no image of the individual is produced but, in case of detecting a threat item, it identifies the area of the body where it has been detected for further search of the passenger by an agent. (see **Figure 2**[2]).

2.3. Sub-Millimetre Wave Scanner SMW

SMW scanners (also named *Terahertz Scanners*) work within the range adjoining MMW between 0.3 and 3 THz, with a wavelength which goes from the infra-red limit (0.1 mm) to microwaves (1mm). A lower wavelength allows production of higher resolution images. However, the capability of penetration through textile fabric is reduced. As with MMW scanners, passive SMW and active SMW scanners have been developed.

To date, MMW technology has had a wider spread than SMW in security applications as, in order to operate in the terahertz frequency range, SMW technology needs more powerful sources of energy (for active scanners) or higher sensitive detectors (for passive scanners) [4]. *ThruVision Systems* provide various passive SMW devices.

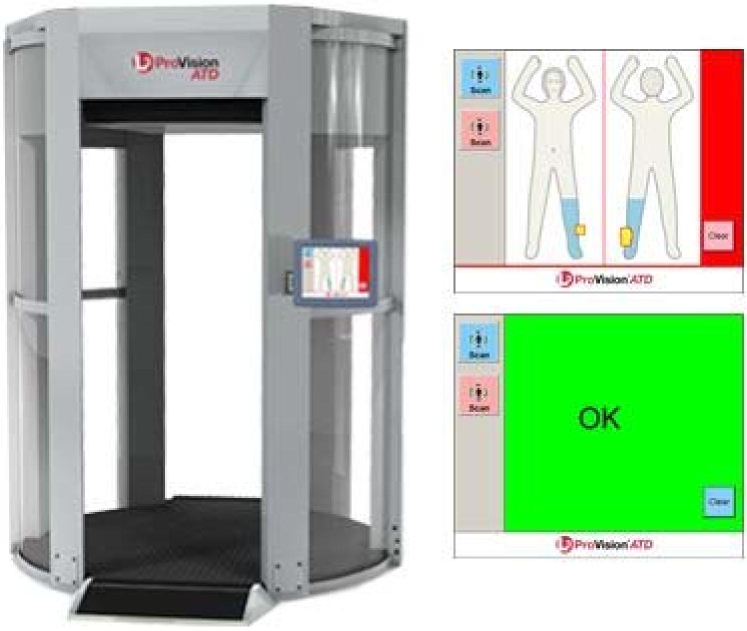


Figure 2. L3 ProVision ATD Scanner. The ATD Software Enhances, on a Human Silhouette, the Areas Where Threat Items Are Detected.

3. Legal Framework

European legislation on civil aviation security is established on Regulation (CE) nº 300/2008 of the European Parliament and the Council of 11 March 2008, *on common rules in the field of civil aviation security*. In this Regulation, the International standards of Annex 17 to the Chicago Convention on International Civil Aviation of 7 December 1944 (Chicago Convention) are adopted as common standards on security.

This rule was later supplemented by Regulation (CE) nº 272/2009 of the European Parliament and of the Council of 2 April 2009, *supplementing the basic common standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 and* by Regulation (EC) nº 185/2010 of the Commission of 4 March 2010, *laying down detailed measures for the implementation of the basic common standards on aviation security.*

Both complementary regulations were amended in November 2011, by other regulations having a special significance to the use of body scanners. Firstly, Commission Regulation (EC) nº 1141/2011, adds a new item to the list of allowed methods of screening: "*security scanners which do not use ionising radiation*". Secondly, Commission Regulation (EC) 1147/2011, which sets the minimum operational conditions on the use of security scanners. In section 5 of this paper we will analyse the aforesaid conditions.

Also of special significance is the Communication COM (2010)/311 [5] that the European Commission produced on 15 June 2010, at the request in 2008 of the European Parliament, in which it urged the Commission to define a specific legal framework on the use of body scanners at EU airports. For this purpose, the Commission raised a consultation to the European Data Protection Supervisor (EDPS), the Article 29 Working Party and to the European Union Agency for Fundamental Rights (FRA). The communication, aiming at establishing a harmonised common framework on the use of scanners, deals with technical equipment issues, passengers´ health protection and users' fundamental data rights.

All European legislation, aviation security included, must comply with the principles set in the Charter of Fundamental Rights of the European Union [6]. In this context, special attention must be brought to the following Fundamental Rights which cannot be interfered with nor limited by the Member States: human dignity, right to the integrity of the person, respect for private and family life, protection of personal data, freedom of thought, conscience and religion; non-discrimination, the rights of the child or freedom of movement. In section 5 of this paper we will cover in detail the impact of body scanners on these fundamental rights.

4. Situation of Body Scanners in Europe

As indicated above, the Communication from the Commission COM (2010)/311 of June 2010, aimed at ending the fragmented situation which existed wherein the various Member States and airports decided if and how to deploy Security Scanners, with the proposal that the use of Security Scanners "*must be based on common standards*", imposing the necessary safeguards to comply with fundamental rights and passengers' health provisions.

Various Member States (France, United Kingdom, Finland, Netherlands, Italy and Germany) have conducted trials of body scanners, with different results which we analyse below.

4.1. France

In February 2010 a Security scanner was tested for three months in terminal 2E at Paris Charles de Gaulle airport. It was a millimetre-wave scanner from the company *VISIOM (French subsidiary of L3 Communications).* The image was analysed in a room located on another floor, by a reviewer of the same gender as the passenger. If a threat item was detected, the security checkpoint agent received an image with a human silhouette indicating in red those parts which had to be verified by a hand search. In no case was the image saved.

Over 8,000 passengers accepted being screened. The results of trials evidenced a good acceptance of scanners by passengers, who considered screening a less intrusive measure than hand searching. However, the French Directorate General of Civil Aviation (DGAC) considered that current technology was not sufficiently mature as to consider an immediate deployment of scanners; it would be necessary to reduce the ratio of false positive results and improve detection of certain items.

The *Comission Nationale de l'Informatique et des Libertés* (CNIL) conducted an on-site inspection of the experimental body scanner installed at Paris airport to verify if its recommendations had been regarded, verifying that: [7]:

- The scanner uses millimetre wave technology, which displayed a generic outline of the human body and not a real image.
- The scanner does not allow saving or copying any images.
- The reviewers are located in an isolated room and do not know the identity of the screened person, so that there is no chance of the passenger being directly or indirectly identified by the image.
- The passenger can choose between undergoing the scanner or a hand pat-down.

From this experience, they agreed to start a three-year trial period for which the CNIL has requested the State Council to pass a decree regulating the operation of these devices (technical conditions, exercise of rights by users, special information and consent rights, conditions for treatment of the images obtained). This new period started at regional airport Nice Côte d'Azur in September 2012, for International flights.

4.2. United Kingdom

At a first stage, body scanners were deployed at Manchester, Heathrow and Gatwick airports. Millimetre wave scanners from the companies *L3 Communications* (model *ProVision*) and *Smiths Detection* (model *Eqo*) are in operation at these three airports. *Backscatter* X-ray scanners were also in operation (*Rapiscan* models *Secure 1000* and *Secure 1000 Single Pose*) but only at Manchester airport.

The scanners were deployed within the common framework of measures to enhance security at British airports, which the Department for Transport introduced after the attempted terrorist attack of Northwest Flight 253 in 2009.

Unlike other countries, in the UK passengers selected for scanning are not permitted to refuse the scan, otherwise they will no be able to fly. British authorities defend this position by arguing that there are no other alternative methods capable of delivering the required levels of security [8]. According to the Department for Transport, the alternative would be a full private search in which the passenger could be asked to remove all or part of his clothing. It is estimated that 1.5 million passengers have been scanned since these measures were introduced, only 12 persons having refused the scan, who were not able to board the plane.

At the same time the scanners were being deployed, the "Code of practice for the Acceptable Use of Security Scanners in an Aviation Security Environment" was published. As concerns privacy, it states that the reviewers must not be able to see the person they are viewing, that the screen is only to be analysed by authorised officers and that procedures shall be established to prevent the capture of any images, including the prohibition of cameras or mobile phones, into the viewing room. It also states that, at the passenger's request, the reviewer shall be of the same gender as the screened person. As concerns data protection, the code states that no scanned image shall be stored, having to be deleted and destroyed after the scanning analysis is completed; it especially compels any facilities on the scanner which could be used to retain, copy or transmit data to be disabled.

Finally, even though the report from the Health Protection Agency - HPA of the British Government concluded that the radiation doses absorbed by the human body (0,02 ìSv) were so low as to be negligible, Manchester Airport respected the Decision from the European Commission and removed the X ray scanners in October 2012, replacing them by five next generation security scanners using radio frequency-based millimetre wave technology from L3 Communications.

At a second stage, body scanners were deployed at Stansted Airport and London City Airport at the end of 2012.

4.3. Finland

In November 2007, Helsinki-Vantaa airport started to test a backscatter scanner with the purpose of using it as an alternative method to hand search during peak hours. The screening, which was conducted on a voluntary basis, was undergone by passengers selected randomly, who were informed of the procedure and had to give their consent prior to the

> "According to the Council of Europe, authorities shall interfere in the right to privacy in an emergency case when it is a question of national security or public order. But, is routine security control at an airport a question of national emergency?"

screening. The person analysing the image was in a separate room with no possibility at all to see or identify the screened person.

One year and a half later, the Finish civil aviation authorities (*Finavia*) decided to withdraw the scanner, just before the Parliament and the European Council prohibited the use of X rays for human controls at airports.

4.4. Netherlands

Schiphol (Amsterdam) airport was the first in the world to deploy security scanners in a 2006, joint initiative of the Dutch customs authorities and the NCTb (National Coordinator for counter-terrorism).

During a first testing period, 17 devices were deployed, which passengers used voluntarily. After the testing period was completed, in May 2007, scanners became part of the airport security system. 60 millimetre-wave scanners from the *L3 Communications*, equipped with ATD (Automated Target Detection) technology, are currently deployed. In this technology a passenger's image is not displayed. Instead, a silhouette of the human body is displayed, ATD software enhancing those areas where the threat item has been detected. However, passengers can always refuse to be scanned and can opt for alternative controls.

4.5. Italy

In 2010 experimental scanners were deployed in Italy at Rome Fiumicino, Milan Malpensa, Venice and Palermo airports. The trials continued in 2011 only at Fiumicino and Malpensa airports. In a press communication of the Civil Aviation National Entity) (ENAC) on 9 February 2012 the experimental period was considered completed and the conclusion was that millimetre-wave scanner technology was the most effective. In particular, the scanners tested at Fiumicino and Malpensa were *L3 Provision ATD* with automatic target detection used by over 50,000 passengers.

After analysis of the testing period results [9], the Inter-ministerial Commission for Air Transport and airport security (CISA) has given the green light for the deployment of this model of scanners at the three Italian airports having regular connections with the United States and Israel: Roma Fiumicino, Milan Malpensa and Venice. When they are fully operational, all passengers must first walk through the metal detector arch, and then through the security scanner. Passengers refusing to undergo the security scanner will be able to opt for alternative methods such as pat-down.

4.6. Germany

Trials were performed at Hamburg Airport with two body scanners between September 2010 and July 2011, where about 809,000 passengers voluntarily underwent such scanning equipment. Both devices used were *L3 Provision ATD* millimetre-wave technology.

After analysis of the testing period results, the German Ministry of Home Affairs dismissed the use of such scanners because it considered that equipment detection reliability did not meet its expectations. The Ministry's report reveals a high ratio of false positive results which is translated into an increase of the amount of time at screening points. However, they do no refuse to take this equipment into consideration in the future when it meets the required security standards and can handle a great number of passengers.

Almost two years after trials at Hamburg Airport, a new trial period was started in November 2012 at Frankfurt Airport. For that purpose, a new generation of body scanners were used, which do not show actual body images but mark the places to be checked by airport staff on a pictogram of a body. Only passengers heading to North America can be required to walk through these scanners.

5. Body Scanners and Privacy

Various European and International entities and organizations have drawn attention to the impact of body scanners on fundamental rights, mainly on privacy, human dignity and data protection, although other rights might also be affected.

The use of scanners that emit ionizing radiations (e.g. X-rays) may violate the rights to physical integrity and health protection. The fact of passengers being compelled to undergo a scan, without being able to opt for alternative methods, entails a restriction of the right to freedom of movement for those refusing the scan. The capability of some devices to reveal a display of a "naked" body on a screen can affect the right of freedom of thought, conscience and religion or the selection of passengers based on criteria such as gender, race, ethnic or social origin, language, disability etc. directly affect the right of non-discrimination.

Any limitation to these rights must respond to principles of necessity and proportionality. According to the Council of Europe, authorities shall interfere in the right to privacy in an emergency case when it is a question of national security or public order. But, is routine security control at an airport a question of national emergency?

The security expert Bruce Schneier [10] argues that the security measures being applied will not stop terrorist threats and, instead, they are a nuisance and entail an invasion on users' privacy. First, metal detectors, then shoe inspection, later prohibition of liquids and finally body scanners. Each time a terrorist attack or an attempt of terrorist attack takes place on a plane, different techniques are used, precisely because terrorists try not to be detected by existing controls. Schneier argues that national security agencies must focus their efforts in detecting the threats before bombers get to the airport

In October 2011, European Data Protection Supervisor (EDPS) sent a letter [11] to the vice-president of the European Commission, responsible for Transport, saying that "use of body scanners is not duly justified when there are less intrusive procedures".

On 14 November 2011, the European Commission decided to adopt the proposal that permits the use of body scanners at EU airports under certain conditions that must safeguard fundamental rights and health protection:

- Prohibition of X-ray scanners.
- Scanners shall not store, retain, copy, print or retrieve images.
- The reviewer analysing the images shall be in a separate room so that the passenger cannot be identified.
- The passenger may request that reviewing of images is undertaken by a person of the same gender.
- The face of the passenger shall be darkened or blurred.
- Passengers shall be informed of the technology being used, of the conditions of use and the possibility of refusing the scan.

Concerning protection of data, the EDPS and the Article 29 Working Party have stood by [12] the opinion that the use of scanners entails data protection treatment and falls into Directive 95/49EC on Data Protection and, therefore, must comply with the principles of necessity and proportionality.

In addition, the Article 29 Working party, has also given its point of view regarding consent. In Opinion 15/2011 of 13 June, on the definition of consent, expresses reservations towards consent given in terms of article 7 of Directive 95/46/EC. As passengers to undergo body scanners have the option to choose alternative methods (hand search, pat down etc.) it could happen that they give their consent to be scanned to avoid delays or other problems, since their objective is not to miss the flight. In consequence, the consent could be considered not to have been freely given.

6. Conclusions

Since some EU Member States started body scanner trials (mostly at the beginning of 2010) several legislative proposals have been progressively passed on civil aviation security, in general, and on use of body scanners, in particular. The different proposals intended, on one hand, to establish common rules on airport security and, on the other hand, to safeguard passengers' fundamental rights and health protection.

Opinions, recommendations, reports or consultations of the main bodies dealing with privacy and data protection (the European Data Protection Supervisor, Article 29 working party and the European Union Agency for Fundamental Rights) have decisively contributed to the definition of such rules.

The approval in November 2011 of Commission Regulations (EC) nº 1141/2011 and nº 1147/2011 set the starting point for the use of body scanners as a legal method for persons' control, and not only as a experimental method as it had been up to that point.

Current rules entail an improvement on safeguarding passengers' rights: X-ray scanners are prohibited; screening is optional and there will be alternative control methods; images shall not be able to be stored or transmitted in any way; passengers shall be informed of the technology used and the conditions of its use.

Despite the aforesaid, there are still questions to be answered. Considering that technologies allowing full automated target detection (ATD) are sufficiently developed, why not let the ATD software inform a human reviewer only when threats may be present? This would absolutely prevent the creation of body images in most cases (passengers concealing nothing) and, only in case of detecting a threat item, the device would show the area to be searched on a general body outline.

On the other hand, it should be noted that bodies such as Article 29 Working Party continue to criticize civil aviation authorities for not been capable of duly justifying the need of such scanners (e.g. with a privacy impact assessment (PIA) [13]). In addition,, the *Electronic Privacy Information Center* (EPIC) in the United States has filed a suit against the Transport Security Authority (TSA) of the *Department of Homeland Security* (DHS) of the American government to suspend the Body Scanner Program at airports [14].

We are facing an ongoing debate between privacy and security. Increasing security measures involves, in contrast, both a limitation on privacy and a nuisance and an inconvenience for the user. [15]. New tendencies in the civil aviation security field intend to avoid such limitations and inconveniences. Although security controls cannot be removed, they should be unified in such a way that passengers could walk through an checkpoint dedicated to security and not have to stop or even take off their coats, boots, belts, watches, mobile phones, luggage etc. Security would be reinforced by intelligence techniques and behaviour analysis. In this context, although not without some objections as far as privacy is concerned, the *International Air Transport Association* (IATA) presented the "*The Checkpoint of the Future*" [16] at the 67 World Air Transport Convention in Singapore (2011), under the motto "*Looks for 'bad people' and not just bad things*".

References

[1] **A. Chalmers**. Three applications of backscatter X-ray imaging technology to homeland defense. *Proceedings of SPIE, Vol. 5778*, pp. 989-993 (2005).

[2] **Health Protection Agency**. *Assessment of comparative ionising radiation doses from the use of rapiscan secure 1000 x-ray backscatter security scanner*. Department for Transport, UK (2010). <http://www.dft.gov.uk/publications/assessment-of-comparative-ionising-radiation-rapiscan-security-scanner>.

[3] **M. Moreno-Moreno, J. Fierrez, J. Ortega-Garcia**. Millimeter- and Submillimeter-Wave imaging technologies for biometric purposes. *XXIV Simposium Nacional de la Unión Científica Internacional de Radio (URSI)*. Santander (2009).

[4] **R. Appleby, R. Anderton**. Millimeter-Wave and Submillimeter-Wave imaging for security and surveillance. *Proceedings of the IEEE, Vol. 95*, pp. 1683-1690 (2007).

[5] **Comisión Europea**. *Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final*. EU (2010). <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0311:FIN:EN:PDF>.

[6] **M. López Escudero *et al***. *Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo*. Fundación BBVA. Bilbao (2008).

[7] **Commission Nationale de l'Informatique et des Libertés**. *Body scanner: quel encadrement en France et en Europe?* Artícle CNIL, Francia (2010-06-08). <http://www.cnil.fr/la-cnil/actualite/article/article/body-scanner-quel-encadrement-en-france-et-en-europe/>.

[8] **The Secretary of Department of Transport (Justine Greening MP)**. *Airport security scanners*. Department for Transport, UK (2011-11-21). <http://www.dft.gov.uk/news/statements/greening-20111121>.

[9] **Ente Nazionalle per l'Aviazione Civile**. *Comunicato stampa: Risultati della sperimentazione dei security scanner (body scanner)*. ENAC, Roma (2012-02-09). <http://195.103.234.163/Applicazioni/comunicati/comunicato.asp?selpa1 =1641>.

[10] **B. Schneier**. *Beyond fear: thinking sensibly about security in an uncertain world*. Copernicus Books, New York (2003).

[11] **European data Protection Supervisor**. *EDPS comments on the draft proposals for a Commission Regulation on common basic standards on civil aviation security as regards the use of security scanners at EU airports*. EDPS (2011-10-17). <http://www.statewatch.org/news/2011/oct/eu-edps-com-body-scanner-opinion.pdf>.

[12] *Ibid.*

[13] **D. Wright, P. De Hert (editors)**. *Privacy Impact Assessment*. Springer, New York (2012).

[14] **Electronic Privacy Information Center**. EPIC v. DHS (Suspension of Body Scanner Program). EPIC microsite. <http://epic.org/privacy/body_scanners/epic_v_dhs _suspension_of_body.html>.

[15] **E. González**. ¿Son eficaces las medidas de seguridad aeroportuaria? Seguritecnia, nº 361. Ed. Borrmart (February 2010).

[16] **K. Dunlap (IATA Director Security & Travel Facilitation)**. *IATA Media Briefing Security*. IATA, 67th Annual General Meeting, Singapore (2011). <http://www.iata.org/pressroom/Documents/security-june-2011.pdf>.

Notes

[1] Figures 1 and 2 have been included and referenced from Section 2 (*Body Scanner Technologies*) only to show to the reader what the equipment (to capture three-dimensional images and human silhouettes, respectively) looks like. Therefore, they are not intended to reflect the actual procedures followed nowadays in the EU airports.

[2] See note 1.