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>
Aragon 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

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).