FONDATION
TELECOM

Think Tank
Futur Numérique

Cahier de prospective

The Futures of Privacy

The Futures of Privacy

Editor
Carine Dartiguepeyrou

ISBN 978-2-915618-25-9

Edition: Uniqueness

Table of contents

Introduction

Cultural Differences in the Perception of Privacy

Global Privacy Governance

Value Creation and Privacy

Conclusion

Introduction

The Challenges of Privacy

Francis Jutand

Privacy is a cultural concept whose definition is connected to social rules establishing what is private or not; in the context of the digital information and communication technologies, privacy determines what behaviors or data must not be watched or spied upon, or what cannot be allowed to be diffused even if the person is aware of the fact. These rules, legal or tacit, are different according to countries, the size of cities, and social classes.

The digital evolution results in new spaces, new networks and new behaviors, mixing traditional rules and new digital rules. It develops a new frame for data and information production, access, exchange or deal.

Data becomes information when its owner gives his consent to someone to access his own data. Data and information knowledge captures parts of a person's behavior. "Personal data" is information one can link to a specific person. "Private data" is data we agree should remain part of the person's privacy. Social agreements may be different about data depending on who is the person concerned; for example some personal data could be agreed to be public when concerning a public person, while being private for an ordinary fellow.

Another question arises when dealing with personal data shared within a group. Some rules, such as rules to control the use of one's name or image, could depend of the size of the group.

But the key question to be dealt with is: Is there an owner for a data? If the answer is yes, then who is the owner, what are the rules of usage of this owned data, and what are the nature of the contract and the terms of consent?

The problems to be solved are not new, they are as old as media. But digital capabilities make some abuses easy; they make data usage evolve and step by step remove the boarders of privacy. Data can be hacked and resulting in identity abuses and faked contents. Diffusion of data, real or faked, can be organised to damage the reputation of people.

But beyond that, the emerging problem is connected with the capacity to use personal data, digital footprints, and tracks of usage. Who is allowed to use this data, the person or the service provider? Can this problem be solved by forty-pages-long contracts, as a way for the user to give their consent?

This global evolution – and what we see now is just the beginning of the digital metamorphosis[1] – is pushed forward by two engines: economy and psycho-sociology.

Big Data technologies give companies power to process huge quantities of data to produce information and knowledge that could become sources of value creation. Selling data could bring in big money, which means there is today a real economics pressure to reduce the limits of privacy. By combining open data, contents of the grey domain (where ownership rules are not clearly defined), private contents (which users give right to use by signing 40-pages contracts), and data resulting from access to Net services, digital operators can create value from data and offer very innovative services. This is the heart of massive digital platforms who offer free services to customers so that they can create value out of customers' access for people interested in selling products, services, or access to other sellers. Creation of knowledge through Big Data, potential innovative services, referencing, advertisement, intelligence activities, there are a lot of very profitable reasons to release the maximum part of personal data from the limits of privacy.

Concurrently there is a kind of psycho-sociological pressure to make open use of personal data: A social pressure and an interest to share data and contents through social networks, but also personal valuation trough public access to personal data. The digital society could evolve toward a kind of transparency about personal data. And rather than a "Big Brother evolution of society" it could favor ideas such as "anyway, some people I don't know have access to my private data, so there is no need to make a difference between private or not private."

Some fear with reasons the Big Brother kind of scenarios, with a disappearing boarder between private and public personal data, with a danger to erode and affect the inner versus outer domains, which are so critical to build up one's own personality. Others claim privacy is an old concept. Still others think we need time to adapt, and that step by step we are going to develop rules and tools to manage and master the privacy issues.

Francis Jutand *serves as Director of the Department of Scientific Affairs and Member of the Board of Governors at the Institute Mines-Télécom. He is President*

[1] See *La métamorphose numérique (The Digital Metamorphosis)*, by F. Jutand and 14 authors on the impact of the digital metamorphosis.

of the ICT Scientific Committee of the ANR and Vice President of the Alliance of Digital Organisations (Allistene). He initiated and is Vice President of the Competitive Pole CAP Digital. Prior to the Institut Mines-Télécom, he was in charge of the ICT department at the CNRS, Scientific Director at France Télécom R&D and Director of Télécom Bretagne, and professor at Télécom ParisTech. He has been actively engaged in futures studies for the last 15 years, a member of Prospective 2100 and has created the "Futur numérique" (Digital Futures) Think Tank at the Institut Mines-Télécom, which focuses on the digital metamorphosis and its impacts on economy, humans and society. He recently initiated and published La Métamorphose numérique (Digital Metamorphosis) *(Alternatives, 2013). He is also a member of the Conseil National du Numérique.*

Sharing our Visions of the Future of Privacy

Carine Dartiguepeyrou

The Privacy Programme was initiated in 2013 with the support of the partners of the Fondation Télécom, i.e. Alcatel-Lucent Bell Labs, BNP Paribas, Google, Orange and SFR.

The first objective was to define the concept of privacy (personal data) and establish some key questions around its likely evolution. The programme conducted by the Think Tank Futur Numérique was radically orientated towards the future with a line of horizon of ten years.

The second objective was to share our visions of the future from the business and research angles. A group of 12 international experts was set up coming from both the corporate world and the Institut Mines-Télécom. The contributors of the working group were:

- Michel Benard, Academic Relations Manager, Google
- Carine Dartiguepeyrou (facilitator), Think Tank Digital Future
- Marie-Pascale Dupont, Alcatel-Lucent Bell Labs
- Thomas Heimann, Researcher, Google
- Francis Jutand, Head of the Department of Scientific Affairs, Institut Mines-Télécom
- Stéphane Lebas, Product Marketing Director, SFR
- Marion Le Gléau, Projet Manager of Dashboard Trust at OLPS, Orange
- Claire Levallois-Barth, Lawyer, Researcher at Télécom ParisTech
- Christian Martin, Institut Mines-Télécom Silicon Valley, Moutain View, California
- Josef Sievers, Manager of Client Experience, SFR
- Matthieu Soulé, Strategy and Foresight, Retail Banking, BNP Paribas
- Vincent Toubiana, Research Engineer, Alcatel-Lucent Bell Labs

Five workshops took place *in situ* and on Google+. The task was not easy as there was the barrier of the language (the working language was English), the barrier of the different experiences (research, future studies, marketing, legal, etc.), as well as a variety of paradigms. The questions addressed were:

• Will **ownership** still be a value worth something in ten years time? Do we need to have "someone who owns" or should we prefer "universal access"? With digital technologies, is this value-rising or, on the opposite, value-declining?

• In ten years time, is public data likely to define our **digital identity**? Will the value of respect still be relevant? Is digital identity likely to overpass personal identity and private life?

• How is **value creation** likely to evolve in the coming ten years? What are the major levers of change? Since service is adding value to data (raw vs aggregated data), how are services likely to evolve? Will usage lead to an increase or decrease of economic intermediaries (economic actors)? As awareness on privacy increases, is public value likely to develop and how? What roles could communities and group of individuals play in providing social value?

Once we had shared our understandings and key questions around this three themes, we then proposed to share our visions of the future. Each member proposed a scenario for 2023. The results were surprising. Although the first workshops showed there were various understandings of the concept of privacy and its likely evolution, the experience of the scenarios showed some convergence.

These were the emerging points of convergence:

• More transactions, more data exchanged, flow brings value (vs stock, vs property); value creation comes from interaction, attracting attention (vs selling data), creating new links, from what you do with it (vs collecting).

• Cognitive evolution: In the context of overflow of information, we remember the context – where we stored the information and the comments – more than the events themselves; for example, we tend to pay more attention to the "Likes" than to the profile.

• Risk of surveillance society (failure of data protection legislation and of privacy enhancing technologies).

• Expected huge technological collapse, security breach or "Black Thursday" in the data ecosystem between 2016 and 2020.

• Traceability and trust, long term relationships, more loyalty to people and business that protect your data; the meaning of trust evolves as value chain creation is often not transparent.

• Double identity online and offline to preserve offline private life.

• Increased acceptance of sharing data for common good, increased social and public value. Likely evolution of the notion of privacy: from "the ability to control one's personal information" (collection, disclosure, use) to "a dynamic process of negotiating personal boundaries in intersubjective relations."

• Personal data as currency of the digital market.

• Different types of business models:

1. Citizens: free for citizens, operated by governments, open data, public value;
2. Clients: ready to pay a premium for integrated solutions and services provided by five key companies (consolidation of the industry);
3. Minority of users who developed their own autonomous solutions.

• A new kind of rights and protection will emerge as data ownership will not mean the same; new legal and technological tools.

The programme was partially presented at Google in Paris by Thomas Heimann and myself on 21st March 2013. It raised great interest and we decided to enlarge the debate by inviting key and inspiring experts in the field. This objective gave birth to the seminar of 17 October 2013 at the Institut Mines-Télécom.

This *Cahier de prospective* is made of contributions and transcripts of participants who gave a talk on the 17 October Seminar.

Carine Dartiguepeyrou, *Coordinator of the Privacy Programme.*
Carine is a futurist, member of the Think Tank Futur numérique at the Institut Mines-Télécom. She leads two programmes for the Fondation Télécom: Corporate Digital Transformation and Privacy. She holds a Msc from the London School of Economics and a Ph.D. in Political Science (Paris 1 Panthéon-Sorbonne). She conducted her post-doctorate at France Télécom R&D. She contributed to several management and societal books focusing on the worldwide mutation and recently to La Métamorphose numérique *(*Digital Metamorphosis, *dir. Francis Jutand, Alternatives, 2013).*

Programme of the seminar 17 October 2013

Opening: Sharing our visions of the future of privacy: a synthesis of the Privacy Prospective Workshops

- **Francis Jutand,** Institut Mines-Télécom, Scientific Director, Member of the Board of Governors at Institut Mines-Télécom
- **Carine Dartiguepeyrou,** Fondation Télécom, coordinator of the "Privacy Programme"

The introduction was dedicated to providing a synthesis of the work that was conducted between November 2012 and March 2013 with the partners of the Fondation Télécom.

First roundtable: Cultural differences in the perception of privacy

What are the differences in the perceptions of what is public and what is private? What are the specifics between the private and public spheres in the digital world? Are there differences between the American, Asian and European perceptions of privacy? What does the political context of a given country tell us? How come the representations of privacy differ more according to individual or group values and behaviours than according to nationalities? Are there specific trends in behaviours, rules and norms that are emerging with regards to privacy? Are the changes in the fields of digital culture, ICT technologies and market offers bringing new insights?

- **Key note speech: Helen Nissenbaum,** Professor of Media, Culture and Communication, and Professor of Computer Science, Steinhardt School of Culture, Education and Human Development, New York University
- **Bregham Dalgliesh,** Associate Professor, College of Arts and Sciences, University of Tokyo; Research Fellow, Interdisciplinary research group ETOS (Ethics, Technologies, Organisations, Society), Institut Mines-Télécom, Paris

Discussion

Introduction of the afternoon session

- **Thibaut Kleiner,** Senior Advisor in charge of Privacy, European Commission Cabinet of Vice-President Neelie Kroes

Second roundtable: Global Privacy Governance

What are the key steps towards achieving a global privacy governance, i.e. even before adopting privacy laws? Which rights should be defended? How do we take into account culture changes such as evolution of values and of social conducts? What are the emerging challenges in America vs Europe vs Asia? What are the needs in terms of elaboration and decision processes with regards to privacy? Are there some specifics? What are the innovative initiatives existing in the field? What are the conditions required to effectively reach a global policy within ten years time?

- **Key note speech: Prof. Wolfgang Schulz,** Media and Law expert, Director, Institute Humboldt HIG Berlin
- **Claire Levallois-Barth,** Maître de conférence; coordinator of the Research Chair Values and Policies of Personal Information at the Institut Mines-Télécom; General Secretary of the French Association of Data Protection Officer (AFCDP)
- **Winston Maxwell,** international lawyer, partner at Hoganlovells
- **Florence Raynal**, Head of European and International Affairs, CNIL
- **Pierre-Emmanuel Struyven,** VP Development and Innovation, SFR

Discussion

Third roundtable: Value creation and privacy

What are the rising questions with regards to privacy, from both the economic and technical perspectives? Can value creation be achieved in this field? What are the existing trade-offs? What are the challenges faced by companies with regards to regulation? How can this be tackled? Which shifts are required, in which fields? What are the likely scenarios in terms of market players? How is their socio-economic contribution likely to evolve in the coming ten years?

- **Key note speech: Nicolas de Cordes,** VP Marketing Vision, Orange
- **Armen Aghasaryan,** Senior Researcher, Alcatel-Lucent Bell Labs
- **Stéphane Lebas,** Marketing Director, SFR
- **Matthieu Soulé,** strategic analyst, Ateliers BNP Paribas
- **Patrick Waelbroeck,** economist, member of the Chair Values and Policies of Personal Information, Institut Mines-Télécom

Discussion

Concluding remarks

Cultural Differences in the Perception of Privacy

Respect for Context as a Benchmark for Privacy Online: What it Is and Isn’t

Helen Nissenbaum

Introduction

In February 2012, the Obama White House unveiled a Privacy Bill of Rights (2012, 9). Although most of its principles were recognizable as a kind of traditional principles of fair information practices, embodied, for example, in the OECD Privacy Guidelines, the third principle of “Respect for Context” (PRC), introduced as the expectation that “companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data” (p. 47), was intriguingly novel. The Report buoyed hopes. It signaled in the White House a serious interest in privacy and it portended a departure from business as usual. In addition to the Bill of Rights, the Framework for Protecting Privacy laid out a multi-stakeholder process, provided foundations for effective enforcement, pledged to draft new privacy legislation, and announced an undertaking to increase interoperability with international efforts to protect privacy (Civil 2012).

At the same time, the dockets of public interest advocacy organisations slowly filled with privacy challenges. Courts and regulatory bodies were awash with cases of overreaching standard practices, embarrassing gaffes, and technical loopholes that enabled surreptitious surveillance and the capture, aggregation, use, and dispersion of personal information. As awareness spread so did annoyance, outrage, and alarm among ordinary users of digital and information technologies, notably, the Web, mobile systems, and location based services.

For anyone following deliberation on the subject of privacy, these observations are not new. More jarring, however, is that this panoply of information practices, for the most part, proceeds under the halo of legality evoking, quite literally, gasps of disbelief, among the newly informed. For privacy scholars and activists, the level of indignation about these perfectly lawful practices adds strength to their position that something in the relevant bodies of law and regulation is amiss, that the *status quo* needs correction. Taking the cue, governmental bodies have begun placing citizens' privacy on their active agenda. It is at this point in the story that my article picks up.

The present moment resembles others in the recent history of privacy in which revelations about new technologies, practices, or institutions push beyond a threshold and momentum gathers for the position that "Something has to be done!" At this juncture, as others, public commentary reflects widespread anxiety over the deployment of IT, networks, and digital and information systems (including so-called "Big Data") that have radically disrupted flows of personal information.[1] It always bears reminding that socio-technical systems embedded in particular political-economic environments and not bare technology are the proper agents of disruption (Nissenbaum 2010). Acknowledging this anxiety, federal authorities have aimed at an adjustment of the *status quo* through such vehicles as the White House and FTC Reports, with similar governmental reactions elsewhere in the world, e.g. WEF Report (2012) and EU Amendments Process. Both Reports include a number of recommendations for policy and procedure, but in this article, as indicated above, the focus is on the White House Consumer Privacy Bill of Rights, and within the Bill of Rights, the Principle of Respect for Context (PRFC), which holds great promise as an agent of change, yet equally, could fizzle to nothing.

1. The White House Report and Respect for Context

The White House Report and its Privacy Bill of Rights were cautiously endorsed by a range of parties who have disagreed with one another on virtually everything else to do with privacy. On the public interest advocacy front, the Electronic Frontier Foundation, for example, which had proposed its own Bill of Privacy Rights for Social Network Users, conceded that, "this user-centred approach to privacy protection is a solid one" (M. Hoffman 2012). The Electronic Privacy Information Center "praised the framework and the President's support for privacy, and said that the challenge ahead would be implementation and enforcement" (EPIC.org 2012), and The Center for Democracy and Technology "welcome[d] the Administration's unveiling," endorsing the Report's "call for the development of consensus rules on

[1] Anxiety over the digital age, and more specifically, Big Data, is a major theme in mainstream tech and business journalism as of 2013. For more information, see *The New York Times*' special section "Big Data 2013." http://bits.blogs.nytimes.com/category/big-data-2013.

emerging privacy issues to be worked out by industry, civil society, and regulators." On the industry front, Google declared itself "on board with Obama's Privacy Bill of Rights," and Intel affirmed the Administration's "[...] calls for US federal privacy legislation based upon the Fair Information Practices" (D. Hoffman 2012).

Unprecedented White House engagement with contemporary privacy problems has buoyed hopes that change is in the air. How far the rallying cry around Respect for Context will push genuine progress, however, is critically dependent on how this principle is interpreted. Context is a mercilessly ambiguous term with potential to be all things to all people. Its meanings range from the colloquial and general to the theorised and specific, from the banal to the exotic, the abstract to the concrete, and shades in between. The positive convergence of views held by longstanding antagonists may be too good to be true if it rests on divergent interpretations. Whether the Privacy Bill of Rights fulfills its promise as a watershed for privacy will depend on which one of these interpretations drives public or private regulators to action.

2. Meanings of "Context"

This article focuses on specific meanings and shades of meanings that seem to have shaped the White House principle, embodied both in deliberations leading up to public release of the Report and in action and commentary that has followed it. My aim is to demonstrate that some interpretations would have no systematic impact on policy and some would lead no further than entrenched business-as-usual. Whereas some meanings offer progressive if limited improvement, an interpretation based on the theory of contextual integrity opens the doors to a genuine advancement in the policy environment, one that heeds the call for innovation, recognises business interests of commercial actors, at the same time placing appropriate constraints on personal information flows for the sake of privacy. I am arguing that only a subset of uses form a viable foundation for systematically shaping privacy policy, and, more importantly, that not all among this subset will mark a productive departure from "business as usual."

In the influential subset, four interpretations are of particular interest; they reflect views of persistent voices in the privacy and IT arena: context as technology system or platform, context as sector or industry, context as business model or practice, and context as social domain.

2.1. Context as technology system or platform

A major instigator of attention to privacy has been the systems of digital networks that form the Internet together with platforms and systems sitting atop (or below) it; most notably, the Web and the host of systems and platforms it, in turn, has spawned. When these systems mediate communication, action, and transaction, we talk of these activities as taking place online, or in Cyberspace, and because of this, it has been natural to conceive of the privacy problems associated with them, tinged with the distinctive character of the medium, as problems associated with the online context, the context of the Net. The language of context as applied to technology slides around quite smoothly, however, and we readily talk of acting and communicating "in the context of a phone call," "in the context of an online social network," "in the contexts of Twitter, Facebook, or Wikipedia," or in the contexts of the various mobile, location-based services and applications.

These expressions suggest that contexts are defined by the properties of respective media, systems, or platforms whose distinctive technical characteristics shape – moderate, magnify, enable – the character of our activities, transactions, and interactions, including ways that information about us is tracked, gathered, analysed, and disseminated. If contexts are understood as defined by properties of technical systems and platforms, then *respecting* contexts will mean adapting policies to these defining properties.

2.2. Context as business model or business practice

Another conception in the discourse surrounding the Report is context as prevailing business model or business practice. According to Google, "the fast-paced introduction of new Internet services drives equally rapid shifts in consumer expectations and preferences. An effective privacy regime must allow for real time reactions to address changes in consumer privacy preferences resulting from the introduction and adoption of new tools and services" (2011, 2). AT&T urges, "this flexibility should also allow companies to describe the use of data within broad categories, such as 'for marketing purposes,' without the need specify the particular purpose for the collection of each piece of data. Indeed, the power of Web 2.0 inter-related media is precisely that content can be used in ways 'that were not expected or understood when they were collected'" (2011, 17).

Interpreted as the model or practice of a particular business, context is established according to that business's aims and the means it chooses to achieve these aims. There is nothing surprising about merchants orienting their buying and selling practices around profitability, so we should not be surprised that information service providers orient their models around growth and a competitive edge. According to this understanding, contexts are defined by particular business models, in turn shaping respective information flow practices. Taking Google's comment above as a concrete case-in-point, this interpretation suggests that contexts generated by their business-driven

Internet services, for example, shape consumer expectations of privacy, and not the other way around.

2.3. Context as sector or industry

Although the schema I have adopted places "industry" in the same category as "sector," it is not because they have identical meanings, but because, in practice, they are used interchangeably in the commentaries that have rendered it. Google's comments are a case in point, praising the Dynamic Privacy Framework because it seeks to "accommodate and defer to enforceable codes of conduct and standards that are developed by individual industries and can be adjusted in cooperative settings to reflect changing practices, technologies and shifting consumer expectations..." (2011, 8). Google also endorses the convening of working groups, "to provide clear guidance on industry-specific measures needed to protect consumer privacy in a particular context or industry, and to update those recommendations as technology evolves" (2011, 9). In short, respect for context would amount to adherence to the set of rules or norms developed by and within respective sectors or industries.

2.4. Context as social domain

According to this interpretation, the meaning of context is social sphere, commonly experienced as a differentiated social world constituted by multiple spheres, each with an internal logic of its own. Forming the foundation of the theory of privacy as contextual integrity, this notion of society constructed of multiple spheres as been formally developed in scholarly works of social theory and philosophy, theorises them under various labels, including, spheres, domains, institutions, fields and so forth.[2] In contemporary US and, undoubtedly, in many other nations and cultures, these spheres include, education, healthcare, politics, religion, family and home life, recreation, commerce, friendship, marketplace, work and more. In general terms, spheres comprise characteristic activities and practices, functions (or roles), aims, purposes, institutional structures, values, and action-governing norms, which may be explicitly expressed in rules or laws, or implicitly understood in conventions, norms, practice or merely in "regular" behavior.

Where privacy fits into this picture is a question that the theory of privacy as contextual integrity has addressed – from the landscape of differentiated social spheres, developing both a definition of privacy, with respect to information, and an account of its importance. To explain why respect for

[2] For a further discussion on spheres, see Nissenbaum, 2010 p. 80, 131, 166-169, 198-200, 240-241.

context, understood as respect for social domains, opens new and significant avenues for the proposed White House policy framework, I have provided a brief excursus into the theory of contextual integrity.

2.4.1. Contextual integrity: descriptive dimension

The heart of our concerns is appropriateness; specifically, technologies, systems, and practices that disturb our sense of privacy are not those that have resulted in losses or control, nor in greater sharing of information, but those that have resulted in *inappropriate* flows of personal information. Inappropriate information flows are those that violate context specific informational norms (from hereon, "informational norms"), belonging to a subclass of general norms governing of respective social contexts. The theory of contextual integrity offers a structured account of these informational norms that aims for descriptive rigor as well as normative clout.

Three key parameters define informational norms: actors, information-types, and transmission principles. They prescribe appropriate flow according to the type of information in question, about whom it is, by whom and to whom it is transmitted, and conditions or constraints under which this transmission takes place. Informational norms are context-relative, or context-specific, because, resting atop a model of a differentiated social world, they cluster around coherent but distinct social contexts. Accordingly, the parameters, too, range over distinct clusters of variables defined, to a large extent, by respective social contexts.

Actors, the first parameter – subject, sender, recipient – are characterised by particular context relevant functions, or roles, as they act in capacities associated with particular roles or functions within contexts. These functions include the perfectly mundane and familiar – physician, nurse, patient, teacher, senator, voter, polling station volunteer, mother, friend, uncle, priest, merchant, customer, congregant, policeman, judge, and, of course, many more. In complex, hierarchical societies, such as the contemporary United States, actors governed by informational norms might be collectives, including institutions, corporations, or clubs. Information type, the second parameter, ranges over variables derived from ontologies that, for the most part, reflect the nature of particular domains. Finally, transmission principle, the third parameter, designates the terms or constraints under which information flows.

By isolating the transmissions principle as an independent variable we can reveal the source of error in the dominant understanding of privacy as a right an information subject has to control information about him or herself (through notice and consent mechanisms, for example). Seen through the lens of contextual integrity, it mistakes one part of the right for the whole; mistakes the transmission principles for the informational norm.

The three parameters – actors, information types, and transmission principles – are independent. None can be reduced to the other two, nor can any one of them carry the full burden of defining privacy expectations, except perhaps when one of two of the parameters is so obviously understood, or tedious to fully specify, that it need not be explicitly mentioned. This is why past efforts to reduce privacy, say, to one class of information or to one transmission principle are doomed to fail.

When actions and practices comport with informational norms, contextual integrity is maintained. But when actions or practices defy expectations by disrupting entrenched, or normative information flows, they violate contextual integrity.

The theory of contextual integrity is a theory of privacy with respect to personal information because it posits that informational norms model privacy expectations; it asserts that when we find people reacting with surprise, annoyance, indignation, and protest that their privacy has been compromised, we will find that informational norms have been contravened, that contextual integrity has been violated.

2.4.2. Contextual integrity: prescription and policy

My claim is that context understood as social domain offers a better chance than the other three for the Principle of Respect for Context to generate positive momentum for meaningful progress in privacy policy and law. The account of social domain assumed by the theory of contextual integrity constitutes a platform for connecting context with privacy through context-specific informational norms, and offers contextual integrity as a model for privacy itself. In order to develop this claim, a few observations concerning the White House Privacy Bill of Rights provide a necessary perspective.

3. Respect for Context and the Consumer Internet Privacy Bill of Rights

The White House Privacy Bill of Rights embodies "fair information practice principles" (FIPPS), as have many codes of privacy before it, both in the US and internationally. Acknowledging this, Appendix B of the Report provides a systematic account of its debt to FIPPS and prior codes in a table that lines up respective principles of the Consumer Privacy Bill of Rights (CPBR) alongside respective principles in the OECD Privacy Guidelines, the DHS Privacy Policy, and APEC Principles (2012, 59).[3] The CPBR principles of Transparency, Security, Access and Accuracy, and Accountability have relatively straight-

[3] "Appendix B: Comparison of the Consumer Privacy Bill of Rights to Other Statements of the Fair Information Practice Principles (FIPPS)", White House Privacy Report 2012.

forward counterparts in the other sets of guidelines, each worthy, in its own right, of in-depth critical analysis.

Here, however, my focus dwells primarily on Respect for Context, which Appendix B shows lining up with Purpose Specification and Use Limitation Principles. I also would like to draw attention to the White House's CPBR principles of Focused Collection and Individual Control, whose counterparts in the OECD Guidelines are listed as Collection Limitation and Use Limitation principles. Although the first pair does not explicitly mention context, I argue that context and how context is interpreted have significant bearing on how these two important principles play out in practice.

The right of Respect for Context is summarised as "a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data" (White House Privacy Report 2012, 55). Its close kin, (i) Purpose Specification and (ii) Use Limitation, summarised in Appendix B, from the OECD Privacy Guidelines, require that, (i) "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with these purposes and as are specified on each occasion of change of purpose" (p. 58); and (ii) "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [purpose specification] except ... (a) with the consent of the data subject; or (b) by the authority of law" (p. 58).

4. A question of interpretation

Thus far, we have argued that fixing an interpretation of the Principle of Respect for Context (PRC) promises substantive meaning for the Consumer Privacy Bill of Rights (CBPR). Achieving the more important aim, however, the aim of materially advancing the state of privacy protection in the US requires that we fix the right interpretation. Only social domain fully answers this need.

Although it is not wrong to say that people may act and transact in contexts shaped by technical systems, it is a mistake to hold that these systems fully account for the meaning of Respect for Context. So doing allows material design to define ethical and political precepts; it allows the powers that shape the technical platforms of our mediated lives not only to affect our moral and political experiences through built constraints and affordances, but further, to place them beyond the pale of normative judgment. Where technical platforms mediate multiple spheres of life, such as those constructed by Facebook and Google (particularly its newly "federated" construct), the need to distinguish technological affordance from moral imperative is even more acute.

Interpreting context as sector or industry overcomes some of the drawbacks of context as business model, because instead of devolving to the self-serving policies of each business, norms of information flow could be guided by a common mission of the collective – ideally, collective best practice. This interpretation also aligns with the US sectoral approach to privacy regulation and legislation, which, at its best, allows for the generation of rules that are sensitive to distinctive contours characteristic of each sector.

Interpreting the Principle of Respect for Context as respect for contextual integrity advances the cause of privacy in two fundamental ways. First, it requires any analysis to account for significant changes in information flows due to changes in socio-technical systems, including institutional information practices. Second, it assesses disruptive flows not only in conventional terms of interests and general moral and political values, but also in terms of context-specific functions, purposes and values. Here, in particular, the interpretation of context given in the theory of contextual integrity offers an additional dimension: context is crucial to protecting privacy, and not just as a passive backdrop against which the interests of affected parties are measured, balanced, and traded off; rather, context contributes independent, substantive landmarks that guide how to take these interests and values into account, namely, for the integrity of the contexts themselves – vibrant marketplace, effective healthcare, sound education, truly democratic governance, and strong, trusting families and friendships.

5. Summary of Findings

For the Consumer Privacy Bill of Rights (CPBR) to meaningfully advance privacy protection beyond its present state, a great deal hangs on how the Principle of Respect for Context (PRC) is interpreted. My evaluation reveals key implications of each conception of context – as business model, as technology, as sector, and as social domain. Respecting context as **business model** offers no prospect of advancement in privacy protection beyond the present state-of-affairs. Citing innovation and service as the drivers behind this interpretation, its proponents are expecting individuals and regulators to sign a blank check allowing businesses to collect, use, and disclose information based solely on exigencies of individual businesses.

Respecting context as **sector** (or industry) fares slightly better as it offers a framework beyond the needs of individual businesses to establish standards and norms. How well this approach meaningfully advances privacy protection beyond the present state depends on how sectors are defined.

Understanding context in purely **technological** terms implies that legitimate expectations should be adjusted to reflect the affordances and constraints of the technical system mediating activity, communication, or transaction. Although systems do afford and constrain in specific ways, identifying these as a normative foundation drains respect for context of moral legitimacy, getting things exactly backwards. Our morally legitimate expectations, shaped by context and other factors, should drive design and define the responsibilities of developers, not the other way around.

Interpreting context as **social domain**, as it is characterised in the theory of contextual integrity, avoids many of the problems associated with the other three. To respect context under this interpretation means to respect contextual integrity, and to respect informational norms that promote general ethical and political values, as well as context specific ends, purposes, and values.

It is worth emphasizing that the ultimate contribution of contextual integrity does not rest with the concept of context, *per se*, but with two core ideas that are fundamentally associated with the overarching framework.

One is the idea that privacy (or informational) norms require the specification of all relevant parameters, including actors (functioning in roles), information types, and transmission principles. Omitting one of these yields rules that are partial and ambiguous.

The second core idea is of context specific ends, purposes and values, which extend the significance of privacy, that is, the appropriate flow of information, beyond the balancing of interests. It exposes the dependency of social, specifically, contextual values on proper information flows and once-and-for-all, reveals the flaw in tying privacy's importance to individual harm alone.

Conclusion

Context may very well be constituted by technology, business practice, and industry sector. It may be constituted by geographic location, relationship, place, space, agreement, culture, religion, and era, and much more, besides. In individual instances, each one could qualify and shape our expectations of how information about ourselves is gathered, used, and disseminated. None of them, however, provides the right level of analysis, or carries the same moral and political weight as social domain. This is the thesis I have defended. Upon its basis, I offer an amendment to the Principle of Respect for Context as it is given in the Consumer Privacy Bill of Rights: *Respect for Context means consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the [social] context in which consumers provide the data.*

Helen Nissenbaum, *Professor of Media, Culture and Communication and Professor of Computer Science, Steinhardt School of Culture, Education and Human Development, New York University. Her fields of research include social, ethical, political dimensions of information technology and new media as well as philosophy of technology. She holds a B.A. Mathematics and Philosophy, University of Witwatersrand, South Africa, a Ph.D. Philosophy, Stanford, and a M.A. Social Sciences in Education, Stanford. She is the author of several books including* Privacy in Context: Technology, Policy and the Integrity of Social Life *(2009)*.

References

18 USC § 2511(2)(a)(i). "Interception and disclosure of wire, oral, or electronic communications prohibited" (2)(a)(i). Available at http://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap119-sec2511/content-detail.html.

Angwin, J. and Valentino-Devries, J. 2012. "New Tracking Frontier: Your License Plates." *The Wall Street Journal*, September 29. Accessed June 12, 2013 from http://online.wsj.com/article/SB10000872396390443995604578004723603576296.html.

Chavez, P. L. 2011. Comments of Google Inc. to US Department of Commerce. Electronic filing, January 28. Accessed June 11, 2013 from http://www.ntia.doc.gov/files/ntia/comments/101214614-0614-01/attachments/FINALCommentsonDepartmentofCommercePrivacyGreenPaper%20%283%29.pdf.

Cate, F. 2006. "The Failure of Fair Information Practice Principles." *Consumer Protection in the Age of the Information Economy*, July 8. Accessed July 1, 2013 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

Civil, C. 2012. "President Obama's Privacy Bill of Rights: Encouraging a Collaborative Process for Digital Privacy Reform." *Berkeley Technology Law Journal*, March 12. Accessed June 11, 2013 from http://btlj.org/2012/03/12/president-obamas-privacy-bill-of-rights-encouraging-a-collaborative-process-for-digital-privacy-reform/.

Department of Commerce and National Telecommunications & Information Administration. 2012. "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." White House Privacy Report, February 23. Accessed June 11, 2013 from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Department of Homeland Security. 2013. "Web Site Privacy Policy." Accessed June 12, 2013 from http://www.dhs.gov/privacy-policy.

Federal Trade Commission. 2012. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers." FTC Report, March. Accessed June 11, 2013 from http://www.ftc.gov/os/2012/03/120326privacyReport.pdf.

Friedman, M. 1970. "The Social Responsibility of Business is to Increase its Profits." *The New York Times Magazine*, September 13. Accessed June 11, 2013 from http://www.colorado.edu/studentgroups/libertarians/issues/friedman-soc-resp-business.html.

Hoffman, D. 2012. "White House Releases Framework for Protecting Privacy in a Networked World." Post on Policy@Intel blog, February 23. Accessed June 12, 2013 from http://blogs.intel.com/policy/2012/02/23/white-house-privacy.

Horan, P. 2011. Re: FTC Staff Preliminary Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers." Online Publishers Association Comments to FTC, February 17. Accessed June 11, 2013 from http://www.ftc.gov/os/comments/privacyReportframework/00315-57664.pdf.

Intel. 2011. RE: FTC Staff Preliminary Report on "Protecting Consumer Privacy." Intel Comments to FTC, January 26. Accessed June 11, 2013 from http://www.ftc.gov/os/comments/privacyReportframework/00246-57451.pdf.

Lawler, B. 2011. Request for Comments: "Information Privacy and Innovation in the Internet Economy." Intuit Comments Before the Department of Commerce, Office of the Secretary National Telecommunications and Information Administration, January 28. Accessed June

11, 2013 from http://www.ntia.doc.gov/files/ntia/comments/101214614-0614-01/attachments/Intuit.pdf.

Maier, F. 2010. TRUSTe's Comments in Response to the Department of Commerce's Green Paper: "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." Electronic filing, January 28. Accessed June 11, 2013 from http://www.docstoc.com/docs/150372462/For-body-font-Preferably-Arial_-11-sized-font---which-is-what-most-of.

National Telecommunications and Information Administration. 2011. Testimony of Assistant Secretary Strickling Regarding the State of Online Consumer Privacy. Transcript, March 16. Accessed June 11, 2013 from http://www.ntia.doc.gov/speechtestimony/2011/testimony-assistant-secretary-strickling-regarding-state-online-consumer-privacy.

National Telecommunications and Information Administration. 2012. "Multistakeholder Process to Develop Consumer Data Privacy Code of Conduct Concerning Mobile Application Transparency." Notice of meeting published by Federal Register, June 28. Accessed June 11, 2013 from https://www.federalregister.gov/articles/2012/06/28/2012-15767/multistakeholder-process-to-develop-consumer-data-privacy-code-of-conduct-concerning-mobile.

Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford, CA: Stanford Law.

Nissenbaum, H. 2011. "A Contextual Approach to Privacy Online." *Daedalus* 140(4): 32-48.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. September 23 1980. Accessed on June 11, 2013 from http://www.oecd.org/Internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Rauhofer, Judith. 2013. "One Step Forward, Two Steps Back: Critical Observations on the Proposed Reform of the EU Data Protection Framework." *Journal of Law and Economic Regulation* 6(1).

Rubinstein, I. 2010. "Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes." *I/S a Journal of Law and Policy for the Information Society* 6(3): 356-423.

Strickling, Lawrence E. Testimony, March 16 2001, before the US Senate Committee on Commerce, Science and Transportation (Regarding the State of Online Consumer Privacy). Text from NTIA, accessed October 24th, 2013 from http://www.ntia.doc.gov/speechtestimony/2011/testimony-assistant-secretary-strickling-regarding-state-online-consumer-privac.

World Economic Forum. "Rethinking Personal Data: Strengthening Trust." 2012. Report, May. Accessed June 11, 2013 from http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf.

Perspectives from Japan on Privacy and the Supervised Society

Bregham Dalgliesh

Introduction

How to think otherwise is the lot of modern – especially French – philosophy. Despite other approaches, such as the insight generated by innovation gurus or the self-made luck of serendipity, the advantage of philosophical juxtaposition is perspectivism. Michel Foucault, for example, expresses astonishment at the limits of his (Western) thought as it runs up against an alien taxonomy. Indeed, such is the incongruity of the classification of animals that Jorge Luis Borges cites from the Chinese encyclopaedia, *Celestial Emporium of Benevolent Knowledge*, that *Les mots et les choses* « *a son lieu de naissance dans [ce] texte [...] [et] le rire qui secoue à sa lecture toutes les familiarités de la pensée* » (Foucault 1966, 3). What confront Foucault are the cultural specificity of his understanding and the historicity of his knowledge, which are enclosed in an *epistēmē* from where it is well nigh impossible to think otherwise. But it is not just because he came from the land of *le même* that Foucault seemed so perplexed by *l'autre*, which French republican conviction excludes. There really are times when one's *habitus* is exposed for what it is, viz., a perspectival set of dispositions, comportments, ideas and emotions, which make no sense elsewhere.

Apart from the historical limits of our interpretative horizons, therefore, the encounters between what *we* do with what *they* do is a means to problematise our thinking.[1] For this reason, I would like to examine the Japanese conception of subjectivity and how it informs debates about privacy, civil society and surveillance. The presumption is that such an inquiry into how

[1] "Is theory, once translated from the West into Japanese, so to speak, renovated or reborn? Or is it displaced onto other intellectual and political horizons?" (Elliott, Katagiri and Sawai 2013, 2).

they are taken up *there* might help us to think differently about the question of privacy *here*. To begin with, section one sketches a view of the subject of privacy. In section two we outline a discourse on the uniqueness of Japanese subjectivity, which is a potential source for thinking differently about privacy. Section three then focuses on Japanese civil society and the spaces of privacy it affords, which allows a contrast with Western accounts of the public-private dichotomy. Finally, in section four we examine the claim that the notion of a "supervised society" might better capture the ocular nature of power in Japan today. We conclude with a discussion of privacy once it is juxtaposed with its manifestation in Japan.

Notes on privacy and the subject of it

Helen Nissenbaum (2010; 2011), who takes the problem of privacy up into contextualised norms that determine the appropriate flow of information, offers a point of entry into the discussion. Although I take privacy across into other modes of subjectivity, a common concern is Nissenbaum's attempt to defend the one from the many. Here, it is the individual who contracts with corporations, organisations or institutions, as it entails a *virtual* contractual relation that makes *future* misuse of information relatively *inconceivable*. Underlying Nissenbaum's approach is a criticism of the ontology of capitalism, which presumes market exchange is fair if contracting occurs under conditions of equality between rational agents. However, injustice arguably persists due to the flawed assumptions about the contractor, *homo economicus*. Although he enjoys an array of liberal rights – manifest, for example, in the choice to divulge personal information when signing up for online membership – *homo economicus* is no more than a "politico-theological legitimation" (Schwarzkopf 2011, 121) of market exchange as fair because seemingly chosen, though not in actual fact.[2]

Against this background, we can follow Alan Westin's (1967) classic definition of privacy as a *claim* by an individual to determine *what* information about herself should be known to others (and, implicitly, *when* the information is to be obtained and *what uses* will be made of it). This claim becomes a right when it is recognised in law or by social convention. In their famous article published in *The Harvard Law Review* in 1890, Louis Brandeis and Samuel D. Warren suggest that as a legal *right* privacy becomes "the right to be let alone," which is possibly how most of us (in the West) understand it, too.

[2] Stefan Schwarzkopf's (2011, 122) point is that the sovereignty of the consumer is an illusion: apart from having no say in establishing the rules of the market game, subjects are limited in their ability to make informed choices by inconsistent preferences, a lack of information and the bias of dominant corporate actors in the decision-making process.

What form might any invasion of privacy as the right to be left alone take? It may range from private information being released into the public realm (as in so-called "revenge porn" [Jacobs 2013], which reveals how consent is dependent upon context and choice a function of trust), decisions being made on our behalf without consent, or data provided in confidence to one institution being sold to another. The concept of privacy implores legislation on behalf of "personal autonomy" (or the right to decide about all "self-regarding actions"); "self-determination" (or the right to control the flow of information about ourselves, even when others demand access to it); "consummatory" claims (or the right to dignity, or privacy as an end that screens one from any spectacle in extreme, compromising or unforeseen circumstances); and "strategic" intent (or the right to secrecy about final intentions and ends, hence privacy as a means to safeguard and promote self-interest) (Rule 2012, 65-66).[3]

What is central is the mediation of the relation between the individual and the state (or a third party that is subject to regulations put in place by the state) through rights. They initially concern the individual's corporeal sovereignty *vis-à-vis* pre-constitutional arbitrary violence, thereafter the various freedoms (of conscience, thought and speech) to be enjoyed without interference by others, and today the radical transformation by technology of subjectivity and the question of privacy itself. The common denominator is the Western subject, who because she authors, knows, decides, creates, imagines, envisions and chooses, is assigned a right to a private, sovereign realm of thought and action. The question is what happens to privacy when there is no "ghost in the machine" (Ryle 1949, 15), or subject, on behalf of whom the right exists?

Outline of a theory of *Nihonjinron*

Wakon yōsai ("Japanese spirit, Western technology"[4]) is at the heart of an essentialist culture of *Nihonjinron*, or "Japaneseness." It dates back to the Heian Period (794-1185) and the first encounters with China, but was typical of the Early Showa Period (1912-1945), too, though as a nationalist reaction against the "Western Other inside Japan."[5] In its Meiji Period (1868-1912)

[3] In these multiple senses, privacy is an "essentially contested concept," with disagreement about what constitutes a legitimate privacy claim, how much privacy is desirable and who should decide these matters (Rule 2012, 66).

[4] In the desire to blend Western technology with Japanese spirit, the underlying assumption is a neutral technology that can be subject to a managed assimilation and integration, without any change to Japanese spirit. Such an instrumental view of technology merits a future critique, especially in respect of surveillance technologies that are radically transformative.

[5] Toson Shimazaki, who realised he had been missing something prior to his discovery of a Rousseauian inner self (Maraldo 1994), stands out as an exception. For Yukichi Fukuzawa

variant, a pure realm of unique Japanese "spirit," or an essentialist identity, is the overseer of a superficial realm of *technē*, of extra-identity. The gist of *Nihonjinron* is that others have no place within Japan, except as a means for the aggrandizement of the end, "Japaneseness" (Sakamoto 1996, 120).[6]

Yet before piecing together the historical fragments of *Nihonjinron*, to what extent can we rely on this discourse? Does it not, like most essentialist narratives, have to deny its genealogical pedigree and the contingency of subjectivity that is articulated in respect of an imagined community? Yoshio Sugimoto (2010) offers a trenchant criticism of the *Nihonjinron* concept, citing ethnic diversity, class stratification, multiculturalism and the liquification of traditional values as evidence that it is a misnomer in Japan today.[7] However, these phenomena have always existed, albeit as marginalised knowledge and submerged struggles. In this sense, *Nihonjinron* has always trumped its rivals, while surveys still reveal the consistent self-perception of the Japanese as conforming to it. Although Sugimoto (2010, 15-16) dismisses this as mere evidence of the continuation of popular stereotypes, the fact is that *Nihonjinron* is constitutive of the Japanese imaginary and shapes the processes of self-formation independently of its historical pedigree or link to essentialist ontology.[8]

With this methodological caveat in mind, subjectivity – or the "organisation of a self-consciousness" (Foucault 1988, 253) – has its origins in two non-Japanese ethical practices, Confucianism and – (Zen) Buddhism. With the

and Keiu Nakamura, unconstrained liberty was "selfishness" (Howland 2002), individuation for Masao Maruyama (1965) was "modern," viz., Western, and ontological differences were climatically determined, as in Tetsuro Watsuji's (1961) concept of *fudō*.

[6] *Nihonjinron* also enjoys external legitimacy. In *The Rules of Sociological Method*, for example, Emile Durkheim says while Japan may borrow Western *technē* and economic and political organisation, "it will not cease to belong to a different species from France and Germany" (Durkheim quoted in Smart 1996, 180). More recently, Robert Bellah (1965) mentions a Japanese narcissistic psyche that is often manifest as a "particularist nationalism," while for Ruth Benedict (1946, 2) in *The Chrysanthemum and the Sword*, the "Japanese are, to the highest degree, […] both militaristic and aesthetic, […] submissive and resentful of being pushed around, loyal and treacherous, […] conservative and hospitable to new ways."

[7] Additional criticisms of the *Nihonjinron* concept include the fact that the historical and political constitution of an ethnic "Japaneseness" is rarely questioned, with the culture that harbours its key traits treated as an organic unity and coincidental with the unified language that the Japanese are pre-programmed to learn. See Sakai (2009).

[8] To be sure, I share Sugimoto's desire to critique the discourse of *Nihonjinrin* (in respect of empirical, methodological and ideological lacunae). However, such an endeavour also has a genealogical side, which seeks to unravel the contingency in those aspects of *Nihonjinron* that are taken to be ontologically necessary. Following Tessa Morris-Suzuki (1998, 4), we must "delve into the categories of thought which underlie concepts of nationhood – the notions of culture, race, ethnicity, civilization, and Japan itself – and discover how these categories have been used in the Japanese context."

former, self-formation develops through fulfilling social roles. Subjectivity is not located within the individual, nor is it any sense a question of autonomy. Indeed, any attempt to demarcate oneself from others is indicative of selfishness, or of the absence of moral identity. With Buddhism, subjectivity is similarly conceived in terms of an extra-corporeal self. But in contradistinction to Confucianism, the essence of subjectivity is its continuation beyond death through reincarnation. Any sense of autonomy is thus a delusion of separateness. It is pure hubris by the human to think it can interrupt a transcendental process, for a moral individual is in unity with all things, not apart from them. Finally, *Nihonjinron* draws on the Japanese cultural practice of the samurai ethic of *seishin* from the Tokugawa Period (1603-1867). Here, loyalty, discipline, obedience and sincerity are the core ingredients of subjectivity. The ideal is a strong self, or *seishin*, forged through severe physical and mental training (Long 2008, 381-382). It produces a bifurcated individual in whom self-discipline abnegates the self in a Nietzschean process of self-overcoming, though not for the purposes of autonomy or freedom, but of pure obedience to the point of self-sacrifice by *seppuku*, or disembowelment.

The *Nihonjinron* discourse explains a society-wide dualist mode of subjectivity (Sugimoto 2010, 2-5). At the level of the individual, subjectivity is not dependent on a *cogito*, personhood or individuality. Instead, it involves *amae* (Doi 1981), which is the psychological inclination to seek emotional satisfaction by prevailing upon and depending on one's superiors, often at the expense of (Western notions of) individuality. Furthermore, the idea of *ganbaru* is dominant, which entails persistence and endurance, even tenacity and dogged determination. It facilitates the denial or over-coming of any concept of subject-centred identity.[9] One consequence is the secondary importance of the concept of the subject. It is the interpersonal relationship itself, or *kanjin*, not the individuals that constitute the relationship; which is the basic unit of analysis (Hamaguchi 1985). If there is any notion of the subject, it is one of *aidagara*, or the extra-corporeal space between individuals (Watsuji 1961). In this sense, the subject

[9] In its imperative form of *ganbatte*, *ganbaru* is heard on a daily basis and carries a sense of "hanging in" and "not giving up." Interestingly, as Allison (1994, 119-121) argues, there are several other synonyms in Japanese for *ganbaru*, but few Japanese words for its opposite. Those that exist, such as *hima* ("free time") or *yoka* ("time to spare"), are pejorative, while foreign words must be imported via the *katakana* syllabary to represent "relaxing" (*rirakkusu*) or "leisure" (*reja*-), which similarly makes them seem exotic and unnatural to a Japanese person. Indeed, such is the pervasiveness of *ganbaru* that it even determines the experience of its opposites. For Kaoru Amanuma (cited in Allison 2010, 120), it explains why work and leisure are experienced in the same way and why the latter can only last a short time, for what pleasure is there in "working hard" to enjoy free time and "hanging in" to efforts to relax? Moreover, leisure is invariably an individual activity, hence a "selfish" activity in that one must take time off from the group, all of which explains frenetic, five day whistle stop holidays, often to the other side of the world.

oscillates between the *uchi* ("inner") and *soto* ("outer") realms, which require a constant Janus-faced switching between one's *honne* ("true core") and *tatemae* ("public expectation") (Bachnik 1986; Rosenberger 1992).[10]

In sum, when subjectivity is non-corporal, yet mediated by the interaction of two bodies (human or social), we might readily call it a virtual subject in reality, for which privacy, as a question of individual autonomy, makes no sense. Why, after all, would anyone claim ownership of ideas, feelings, emotions, thoughts, preferences or personal information, which is the condition of possibility for the right to privacy, if they are only ever extra-corporeally constituted in face-to-face interaction, the community or language?[11]

Japanese civil society and the spaces of privacy

What are the connotations for privacy in public space of a virtual subject situated in reality? Notions of *ohoyake* ("publicness") in Japan have evolved as a spin-off of centralised power. Initially, the key distinction was that of size: *ohoyake* was a large public space and *woyake* a smaller version. It was only after the adoption of Chinese law in the 8th century, which already distinguished between private and public, that Japan's constitution recognised the concept of *watakushi* ("privateness"), though always in relation to the centralised power system of the day (Deguchi 2013, 57-58).

One effect of the historical dependence of a private sphere on state leverage is that most civil society organisations in Japan have few full-time members (38% have none at all), a small number of full-time staff (on average 20) operate on a small budget and are restricted in influence to regional activity. Furthermore, through the Civil Code (1986) and Nonprofit Organisation Law (1998), the state restricts civil society organisations to public interest functions and discourages them from influencing policy making (Kawato, Pekkanen and Yamamoto 2011, 117-121). On the face of this, there seems to be a curtailment of civic engagement. However, 92% of Japanese citizens belong to one of the 300,000 *choukai* or Neighbourhood Associations (NHAs), which suggests once again that privacy is dealt with in a different manner. Indeed, NHAs have been vital to the democratisation of post-war Japan as

[10] In respect of the latter, interaction at the level of community is oriented around the creation of harmony, which requires careful cultivation and maintenance of relations between superiors and inferiors. These in turn are a function of the length of one's membership of the community, with strong interpersonal ties being cultivated within one's hierarchical chain of command, such that vertical loyalties are paramount.

[11] Hiroshi Kojima (1998) imagines a two-level self, a "serial I" that demarcates itself form its body and is constituted through interaction, and a "primal I" that experiences itself as (an egotistical) centre of the world. Both, however, are mediated via a reciprocal relation with a "you."

real sources of grass-roots democracy and decision-making. Although NHAs enjoyed a renaissance during the Meiji Period (1868-1912) for mutual-aid projects and bio-political administration, historically they have been hierarchical and deployed as a mechanism to infiltrate the home for revenue collection, the imposition of sanctions or the distribution of wartime rations. But since the 1950s NHAs have been instrumental in the process of democratisation. They have abandoned their hierarchical organisation for horizontal structures and diversified their membership (Haddad 2011).

If privacy is *collectively* played out at the level of NHAs, which to all intents and purposes demarcates a space that is off-limits to the state, what is the position of the publicly oriented citizen? Interestingly, while the Japanese word for citizen, *shimin*, enjoys widespread usage, it is tainted with foreign connotations as a universal, interpretative etic concept. Consequently, a particular, subjective emic vernacular concept of citizenship, *seikatsu*, is used.[12] It approximates better to intuitions about what citizenship involves (Sugimoto 2010, 288). How then does the *seikatsusha*, or citizen, manage to bridge the private and public spheres? Takeo Doi (1981), for example, similarly speaks of a Janus-faced subject, the *omote* ("front") that interacts with others in a public sphere, and the *ura* ("back"), who is private. We see that *seikatsu* has evolved from its classical Chinese connotation of (social) life and (material) existence to its contemporary rendering as "everyday livelihood" (or, in Arendtian overtures, *vita activa*, in contradistinction to material and biological aspects of living, or *homo faber* and *animal laborans,* respectively). Today's Japanese *seikatsusha*, or citizen, is an ethico-political animal that constructs a series of autonomous spheres (from government interference and market forces) in which to pursue everything from consumption and recreation to work and quality of life issues (Seifert 2007). In other words, it is through local activist NHAs, which are a heterogeneous ensemble of co-operative groups that seemingly require no surveillance, that Japanese citizens will express their civil engagement.

Surveillance for the few, supervision for the many

It is around questions of surveillance that we can return to the concept of *Nihonjinron*. Although it had underpinned the imperial fascist culture of anti-individualistic collectivism and patriarchal discourse, criticism of *Nihonjinron* was difficult as it implied putting in question the *tennō* (divine emperor) system, which is the only institutional remnant left from the Early Showa Period (1912-1945) (Abe 2000, 56). Notwithstanding, it was difficult after 1945 to deploy a culture of *Nihonjinron* to relaunch modernisation, which started with

[12] For discussion of the emic-etic distinction in respect of Japan, see Harumi Befu (1989).

the American imposition of liberal democracy and rapid industrialisation and urbanisation (Elliott, Katagiri and Sawai 2013, 3-5). In fact, *Nihonjinron* only resurfaced two decades later in the guise of technology. Championed by the government from the 1970s, the information society allowed a reshaping of the imaginary through the technological. Furthermore, it was politically acceptable to Japan's East Asian neighbours, as technology was seen as "culturally neutral and harmless," while the opportunity to become a high-tech ICT device society acted as a socio-psychological compensation for Japan's enforced "cultural inferiority and lack of self-confidence" (Abe 2000, 57).

Consequently, because of Japanese innovations and the bubble economy of the 1980s, the information society flourished. Corporations provided differentiated products, which carried a sign – as well as an exchange – value. Meaning was combined with functionality and cost in Japanese consumer ICT devices. Under a corporate culture of specialisation introduced through technological saturation, a Japanese post-modern culture appeared that was historically and existentially distinct from any notions of *Nihonjinron* (Clammer 1997). In addition, among the younger generation at least, processes of self-formation increasingly passed through the semiotic mechanisms of informational consumerism. Subjectivity came to be expressed through the consumption of the meaning of the commodified sign.

In many respects, therefore, post-modern Japanese culture is not only radically symbolic, but founded on identity as difference. This in turn makes control all the more sinister; the inhabitants of Japan's urban borderlands neither historically nor ethnically belong to the post-modern techno-culture, which facilitates their control. At the same time, membership of this techno-culture is off-limits to most non-Japanese people, because only a linguistically and ethnically hermetic "inner public" (Abe 2000, 62) can recognise the symbolic value of commodified subjectivity. It fosters a heterogeneous, albeit exclusive, Japanese techno-culture on the bedrock of ethnic homogeneity. Ironically, therefore, whereas the economic logic of "informationlisation" is to undercut the nation-state (Castells 1996), in Japan its cultural and political logic has functioned as a "societal control system that legitimates the nation-state" (Abe 2000, 64).

The information society in Japan is therefore technological and political. It also acts as the conduit for the articulation of a new strategically constructed imaginary of *Nihonjinron* (Harootunian 1988). It includes the expression of nationalism in a technological rather than cultural idiom of superiority, which supposes a unique ability to copy and miniaturise. Indeed, such has been the success of this technologically grounded *Nihonjinron* that those outside buy into the perception of "techno-orientalism," too (Morley and Robins 1995). The downside is the strategically targeted surveillance it produces.

In other words, Japan has not entirely fended off the "world-historical transformation [...] of the emergence of new practices, dynamics, and technologies of surveillance" (Haggerty 2009, ix). In Tokyo, for example, surveillance at a glance seems innocuous. The Tokyo Metropolitan Government (TMG) and a high profile governor – below which are 23 *ku* (wards) – govern the city. One level below are the NHAs mentioned earlier and shopkeepers' associations, or *shoutenkai* (SKAs). While formal policing is shared between the National Police Agency (NPA) and the Tokyo Metropolitan Police Authority, there are only 363 NPA cameras in Japan because local government, private corporations and NHAs and SKAs (Murakami Wood 2012, 87) operate the majority. To be sure, camera surveillance has increased due to several events: the Aum Shinrikyo gas attacks on the Tokyo metro in 1996; the 2002 FIFA World Cup, where surveillance mirrored British and American "ideologies of crime prevention" (McGrath 2004, ch. 1) and targeted foreign hooligans and illegal – foreign – vendors; and the Community Security and Safety Development Ordinance of 2003 introduced by the TMG governor in a bid to crack down on crime and its supposed cause, foreigners. In addition, since 2012 all foreign nationals are "dividualised" via an obligatory local resident's registry (*jyuminhyo*), which is digitised and connected to the state's *juki-net* database (Ogasawara 2008).[13] Nonetheless, there has not been a centralisation of control in Tokyo, but the "responsibilisation" of the various actors that deploy it (Murakami Wood 2012, 88).

The effect is the surveillance of the few who do not measure up to the *Nihonjinron* techno-cultural benchmark. In some respects it is a pragmatic issue. Blanket surveillance in Tokyo is difficult due to its panoply of narrow alleyways, while each ward is often financially or politically unable to implement surveillance cameras. Yet strategic surveillance is also political. It follows a logic outlined by Zygmunt Bauman in *Globalisation: The Human Consequences*, in which he distinguishes between the tourist and the vagabond. At the global level, the tourist that searches for new experiences adopts strategies of movement. These take advantage of privileged rights of passage in an exclusive world of time divorced from space. At the other extreme, the tourist's alter ego, the vagabond, precisely because of the absence of any privileges, pursues strategies of survival to escape the ever present threat of "stigmatising" and assignment to the "underclass," which is an anonymous human mass to be dealt with by any means possible (Bauman 1998, 96-97).

[13] As Gilles Deleuze (1995, 181-182) shows, control societies that deploy the mechanism of surveillance constitute new ocular objects, or the "dividual," whose freedom of movement and right of association in the public sphere is dependent on the functioning of their electronic card, which in turn is a function of a smoothly running and anonymous computer system.

The tourists might be said to correspond to the Japanese citizen and the vagabond to the non-Japanese resident. Moreover, the techniques of stigmatising follow an onto-technological logic. On the one hand, the vagabond is the target of a strategic technological intent (Western *technē* guided by Japanese spirit), or surveillance and exclusion from the technological devices that constitute the identity of the Japanese domestic tourist. On the other hand, the tourist is the target and effect of the unintentional effects of ICT (Japanese spirit constituted by Western *technē*). Technologies here are technologies of power in the double sense that they divide and conquer: division insofar as they create difference within (Japanese) sameness; and conquering to the extent that the technologically mediated sign of difference is off-limits to the vagabond, who is subject to domination by surveillance proper. For these reasons, we might speak of the strategic surveillance of the few, the vagabonds, and the supervision of the many, the tourists, via "friendly authoritarianism." According to Sugimoto (2010, 290-291), it "is authoritarian to the extent that it encourages each member of society to internalise and share the value system which regards control and regimentation as natural, and to accept the instructions and orders of people in superordinate positions without questioning."

In terms of "authoritarianism," this discipline-control system employs four main mechanisms of micro-management: firstly, the use of small groups, such as NHAs, as the basis of mutual surveillance and deterrence of deviant behaviour; secondly, an extensive range of mechanisms in which power is made highly visible and tangible; thirdly, the legitimisation of various codes in such a way that superordinates use ambiguities to their advantage; and, fourth, the inculcation of moralistic ideology into the psyche of every individual with a particular stress upon minute and trivial details. However, the administering of these authoritarian mechanisms is "friendly." Firstly, it resorts, wherever possible, to positive inducements rather than negative sanctions to encourage competition to conform; secondly, it portrays individuals and groups in power positions as congenial and benevolent, and uses socialization channels for subordinates to pay voluntary respect to them; thirdly, it propagates the ideology of equality and the notion of a unique national homogeneity, ensuring that notions of difference are blurred; finally, it relies upon leisurely and amusing entertainment, such as songs, visual arts and festivals, to make sure that authority infiltrates without obvious pains. In this light, the predictions at the dawn of the information society of Japanese critical theorist, Masakuni Kitazawa, are poignant. He feared the technocratic bio-politics of a discipline-control state would create a *kanri shakai*, or "supervised society," that is "administered through highly sophisticated mechanisms for forecasting, planning and control… [and which propagate] a set of optimum conditions for that society's well-being" (Kitazawa quoted in Buckley 1993, 415).

Conclusion

Through a broad excursus of the Japanese concept of *Nihonjinron*, we can see that any regulation of privacy, public space and surveillance by international organisations expounding universal norms would merely proliferate the perception of globalisation as a process of westernisation. It would not only be at the expense of the diverse manner in which privacy is practiced, but its Western concept of subjectivity would make a legal framework grounded in the individual nothing more than a proxy for the ravages of transnational capitalism.

It is for these reasons that juxtaposing how privacy is taken up in Japan is important. It provides the opportunity to problematise the subject, which portends well if privacy is to have multiple futures. In short, because of the Japanese extra-corporeal subject in reality, the ontological upheavals of a dynamic of surveillance focused on "digital personae" (Lyon 2001, 15) with "virtual / informational profiles" (Haggerty and Richardson 2006, 4) promises to be of less importance in Japan than in those cultures where subject-centred identity means the individual risks ejection from the landscape of self-identity. With the current "restructuring […] [of] the nature of the individual" (Poster 1990, 185-190), it is possible that we have much to learn from *them* about how to be in the future, where privacy promises to be very different from what it is today.

Bregham Dalgliesh. *After completing his graduate studies in Canada (University of British Columbia) and Scotland (University of Edinburgh), Bregham Dalgliesh taught in France (Sciences Po Paris, Télécom École de Management, ENSTA ParisTech, ESSEC, New York University in France) from 2002 to 2011 before taking up his current position as Associate Professor at the University of Tokyo. He has published widely, with the task of critique taken up through an engagement with science and technology as socially embedded enterprises that demand philosophical reflection because of their constitutive effect upon the politics, culture and ethico-moral relations that define and limit the human condition.*

References

Abe, Kiyoshi. 2000. "The Information Society without Others: A Critique of 'Informatization' in Japan." *Kwansei Gakuin University Social Sciences Review* 5, 53-73.

Allison, Anne. 1994. *Nightwork: sexuality, leisure, and corporate masculinity in a Tokyo hostess club.* Chicago: University of Chicago Press.

Bachnik, J. M. 1992. "Kejime: Defining a Shifting Self in Multiple Organisational Modes." In N. R. Rosenberger (ed.) *Japanese Sense of Self*. Cambridge University Press, 151-172.

Bauman, Zygmunt. 1998. *Globalization: The Human Consequences*. New York: Columbia University Press.

Befu, Harumi. 1989. "The emic-etic distinction and its significance for Japanese studies." In Yoshio Sugimoto and Ross Mouer (eds.) *Constructs for Understanding Japan*. London: Kegan Paul International, 323-343.

Bellah, Robert N. 1965. "Japan's Cultural Identity: some Reflections on the Work of Watsuji Tetsuro." *The Journal of Asian Studies* 24 (4), 573-594.

Benedict, Ruth. 1946. *The Chrysanthemum and the Sword: Patterns of Japanese Culture*. New York: New American Library.

Buckley, Sandra. 1993. "Altered States: The Body-Politics of 'Being-Woman'." In Andrew Gordon (ed.) *Postwar Japan as History*. Berkeley: University of California Press, ch. 13.

Castells, Manuel. 1996. *The Rise of the Network Society, The Information Age: Economy, Society and Culture* Vol. I. Cambridge, MA. and Oxford, UK: Blackwell.

Clammer, J. 1997. *Contemporary Urban Japan*. Oxford: Blackwell.

Deguchi, Takeshi. 2013. "Critical Theory and its Development in Post-War Japanese Sociology: Pursuing True Democracy in Rapid Capitalist Modernization." In Anthony Elliott, Masataka Katagiri and Atsushi Sawai (eds.) *Routledge Companion to Contemporary Japanese Social Theory*. New York and London: Routledge, 40-66.

Deleuze, Gilles. 1995. *Negotiations, 1972-1990*. Trans. Martin Joughin. New York: Columbia University Press.

Doi, Takeo. 1981. *The anatomy of dependence*. Trans. John Bester. Tokyo and New York: Kodansha International.

Elliott, Anthony, Katagiri, Masataka and Sawai, Atsushi. 2013. "Editor's Introduction." In Anthony Elliott, Masataka Katagiri and Atsushi Sawai (eds.) *Routledge Companion to Contemporary Japanese Social Theory*. New York and London: Routledge, 1-13.

Foucault, Michel. 1966. *Les mots et les choses: une archéologie des sciences humaines*. Paris: Gallimard.

Foucault, Michel. 1988. *Politics, Philosophy, Culture: Interviews and Other Writings 1977-1984*. Ed. and introd. L. D. Kritzman and trans. A. Sheridan et al. New York and London: Routledge.

Haddad, Mary Alice. 2011. "Volunteer organisations (re)making democracy in Japan." In Alisa Gaunder (ed.) *The Routledge Handbook of Japanese Politics*. New York: Routledge, 140-151.

Haggerty, Kevin D. 2009. "Surveillance and Political Problems." In S. Hier and J. Greenberg (eds.) *Surveillance: Power, Problems and Politics*. Vancouver: University of British Columbia Press, ix-xviii.

Haggerty, Kevin D. and Ericson, Richard V. 2006. "The New Politics of Surveillance and Visibility." In Kevin D. Haggerty and Richard V. Ericson (eds.) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press, 3-34.

Hamaguchi, Eshun. 1985. "A contextual model of the Japanese: Toward a methodological innovation in Japanese Studies." *Journal of Japanese Studies* 1 (2), 289-321.

Harootunian, Harry. 1988. *Things Seen and Unseen: Discourse and Ideology in Tokugawa Nativism*. Chicago: University of Chicago Press.

Howland, D. R. 2002. *Translating the West: Language and Political Reason in Nineteenth Century Japan*. Honolulu: University of Hawaii Press.

Jacobs, Holly. 2013. "Victims of revenge porn deserve real protection." *The Guardian*, 8 October.

Kawato, Yuko, Pekkanen, Robert and Yamamoto, Hidehiro. 2011. "State and Civil Society in Japan." In Alisa Gaunder (ed.) *The Routledge Handbook of Japanese Politics*. New York: Routledge, 117-129.

Kojima, Hiroshi. 1998. "On the semantic duplicity of the first person pronoun 'I'." *Continental Philosophy Review* 31 (3), 307-320.

Long, Susan Orpett. 2005. "Constrained Person and Creative Agent: A Dying Student's Narrative of Self and Others." In Jennifer Robertson (ed.) *A Companion to the Anthropology of Japan*. Malden, Mass. and Oxford: Blackwell Publishing, 380-399.

Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Maraldo, J. 1994. "Rousseau, Hakuseki, and Hakuin: Paradigms of Self in Three Autobiographies. In R. Ames (ed.) *Self as Person in Asian Theory and Practice*. Albany: State University of New York, 57-82.

Maruyama, Masao. 1985. "Patterns of Individuation and the Case of Japan: a Conceptual Scene." In M. B. Jansen (ed.) *Changing Japanese Attitudes Toward Modernization*. Princeton: Princeton University Press, 489-531.

McGrath, John E. 2004. *Loving Big Brother: Performance, privacy and surveillance space*. London and New York: Routledge.

Morley, David and Robins, Kevin. 1995. *Spaces of Identity: Global Media, Electronic Landscapes and Cultural Boundaries*. London: Routledge.

Morris-Suzuki, Tessa. 1998. *Re-Inventing Japan: Time, Space, Nation*. New York: M. E. Sharpe.

Murakami Wood, David. 2012. "Cameras in context: A comparison of the place of video surveillance in Japan and Brazil." In Aaron Doyle, Randy Lippert and David Lyon (eds.) *Eyes Everywhere: The global growth of camera surveillance*. New York and London: Routledge, 83-99.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Nissenbaum, Helen. 2011. "A Contextual Approach to Privacy Online." *Dædalus, the Journal of the American Academy of Arts & Sciences* 140 (4) Fall, 32-48.

Ogasawara, Midori. 2008. "A tale of the colonial age, or the banner of new tyranny? National identification card systems in Japan." In Colin. J. Bennett and David Lyon (eds.) P*laying the Identity Card: surveillance, security and identification in global perspective*. London and New York: Routledge, ch. 6.

Poster, Mark. 1990. *The Mode of Information: Poststructuralism and Social Context*. Chicago: University of Chicago Press Chicago.

Rosenberger, N. R. 1992. "Introduction." In N. R. Rosenberger (ed.) *Japanese Sense of Self.* Cambridge: Cambridge University Press, 1-20.

Rule, James B. 2012. "'Needs' for surveillance and the movement to protect privcacy." In Kristie Ball, Kevin D. Haggerty and David Lyon (eds.) *The Routledge Handbook of Surveillance Studies*. New York: Routledge, 64-71.

Ryle, Gilbert. 1949. *The Concept of Mind*. Chicago: The University of Chicago Press.

Sakai, Naoki. 2009. "Nihonjinron." In Sandra Buckley (ed.) *Encyclopedia of Contemporary Japanese Culture*. London and New York: Routledge, 356-357.

Sakamoto, Rumi. 1996, "Japan, Hybridity and the Creation of Colonialist Discourse." *Theory, Culture & Society* 13 (3), 113-128.

Seifert, Wolfgang. 2007. "Seikatsu/seikatsusha." In G. Ritzer (ed.) *The Blackwell Encyclopedia of Sociology*, vol. VIII. Malden, Mass. and Oxford: Blackwell Publishing, 4150-4154.

Sugimoto, Yoshio. 2010. *An Introduction to Japanese Society.* Cambridge: Cambridge University Press.

Schwarzkopf, Stefan. 2011. "The Political Theology of Consumer Sovereignty: Towards an Ontology of Consumer Society." *Theory, Culture & Society* 28 (3), 106-129.

Watsuji, Tetsuro. 1961. *Climate and Culture*. Trans. Geoffrey Bownas. New York: Greenwood Press.

Westin, Alan. 1967. *Privacy and Freedom*. New York: Arheneum.

Global Privacy Governance

Introduction[1]

Wolfgang Schulz

The concept of "privacy"

I will start with framing what "privacy" actually is from my perspective. I am an expert in constitutional law, thus I'm interested in the scope of the legal protection of human rights and so on; when you do that, different constitutional guarantees pop up, like data protection, the "right to be left alone," the right to have your own "self-portrayal" in the way you want to have it in the public sphere, and so on.

As for me the baseline is autonomy. The concept of autonomy as "self-determination as regards your personal life" is the base of privacy. I believe – but that of course is open to discussion – that it can serve as a concept for different cultural approaches as well. We have learnt things about the Buddhist approach today, for example, that one could assume that there is no "self" as it has been framed in Western philosophy, so autonomy as a concept doesn't make sense. But if you have a closer look at it, then you will see that things like mindfulness in Buddhist theory have very much to do with autonomy, at least with the aspect of getting rid of determination from others, etc.

I personally believe that autonomy is the core, the basic concept you have to contemplate when it comes to the future regulations of privacy. Having said that, one has to see that contemplating about privacy cannot stop at that point.

A notion which you can hear very often in data protection debates and which has been discussed for a couple of years now, is the "Right to be forgotten." That sounds great – it reminds us of these US movies where you have a memory eraser, and you can just press on a button and nobody knows anymore what you've done, your sins from yesterday are erased, etc. However,

[1] Transcription of the speech given during the Privacy seminar of Institut Mines-Télécom.

we should ponder about the connection between autonomy and memory and when doing so recall one saying by the German sociologist Niklas Luhmann, "Forgetting is the main function of memory." When we think about forgetting and the "right to be forgotten" in the public sphere then we talk about things like social memory. Can there really be an individual autonomy over social memory? Of course, a politician who went astray would like that, to have memories of bribery or other deeds erased, and we know a lot of cases in the online sphere where a person demands archive content which deals with his past behaviour to be taken down. Legal debates revolve around these issues, that people want things to be erased and that means of course, that somehow our social memory is affected.

When we talk about things like that and when we look at the freedom of communication aspect only, we have to see that there is an ambivalence in the concept of privacy: On the one hand, privacy enables communication, because when you know that your privacy is protected in the process of communication, then you contribute to the public debate more openly. On the other hand, autonomy cannot be the only principle governing public communication. You can say that the whole media system is a system that is about social memory and about forgetting things. The news of today erases somehow the news of yesterday.

Intervening with this kind of systems we put in place to create social memory, means on the other hand to interfere with these instruments, the social institutions we have developed. It is up to the media system to structure public memory. That's an interesting freedom of speech issue, I'm intending to do more work on it in the future.

Structural risks for privacy

I now want to talk about a risk we can see already, and a risk we face in future. When we talk about risks, I believe it is important to see what conflict we are looking at. There are actually at least three types of conflicts when we talk about communication in the Internet.

1. We still have individual citizen vs state conflict, and of course the NSA debate we have right now, which is still rather intense here in Europe, at least in Germany, highlights that. This problem has made apparent that this conflict is still a conflict between the private sphere, privacy and the states' interests in security.

2. We have an increasingly important issue, when we talk about privacy, with intermediaries like Google, Facebook and others, the business model of which partly rely on data, on information about personal sphere; at the same time people make use of those intermediaries when designing their "digital self" and relating with others, and deciding autonomously what personal information to give to others and what to restrict somehow.

3. Then of course there are other third parties involved; one of the most important issue being that right holders need their personal data to sue alleged copyright infringers.

I think it is helpful to keep in mind that there are at least these three categories of conflicts, and that we are very likely to them in future, in the next couple of years even. Each type of conflict might call for a specific regulatory solution.

What potential risks do we face and have to deal with when we try to come up with solutions, when we look for a global governance concept for privacy for the next ten years? I list here just some trends:

- Personal data as a payment for services,
- Data as warfare,
- Knowledge asymmetries,
- Recombination of Big Data,
- Blurring of the private-public distinction,
- Informed consent fallacy,
- Data literacy,
- Fragmented regulation and forum shopping.

Personal data is more and more becoming a kind of currency for online commerce. It somehow changes the perspective significantly since many legal systems frame personal rights in a way that comes from human dignity, from autonomy like I mentioned before. The current data protection regulation does not really see personal data as a kind of payment; however, in the everyday life it is.

We see that data can be a kind of weapon, that we need data to fight terrorism for example, and the other way round: information about personal things can be used as a kind of weapon both ways.

Another relevant set of problems link to information asymmetries. When I wear Google Glasses, to take an example, and I look at someone, I receive information about his educational background, what texts he has recently posted online, what his skills are, then there is an inherent asymmetry when he does not wear the same type of glasses. We will see more of this kind of asymmetries in various social situations with the increasing market penetration of augmented reality applications. How do we deal with that?

Another salient issue is Big Data: Many things we have designed to protect private life, to make communication anonymous, don't really work anymore when you have the potential to recombine Big Data, and then detect who the acting individual actually is.

Furthermore, the private-public distinction is blurring. With the social media for example, we get things that colleagues of mine call "private public spheres." There is of course a contradiction in terms, and it is intended to be, and it means that you can create your own individual "public." When laws refer to a public-private distinction, what does it mean in consideration of this grey zone, of the new shades of grey we get here in between the realms of the private and of the public?

Another topic to discuss is the concept of "informed consent," which has become a cornerstone of data protection in Europe. I personally believe that in many cases it is just a smoke screen – it has nothing to do with protecting autonomy, it is just clicking two hundred pages of standard form contract that Apple or whoever puts forward. When I need a new app, I – even as a lawyer – do not read a hundred pages, I just click. I want this app and have it done. This has nothing to do with informed consent. We can call it consent because we consent somehow to opt-in into the legal system that Apple designed. So, in a way it is informed consent, it is informed, but not in the way we used to assume as lawyers, when one really explicitly consents to a legal term: "This legal term, this sentence, this rule shall apply to me, I opt-in." But I don't do that in the cases I mentioned, I opt into a set of privately set norms and I think that's something that needs more research.

Data literacy is another interesting point related to the aforementioned issue: Do people really know what they are doing? Definitely not. As far as I'm concerned, I'm really blind, to some aspects at least.

The last point in my list is an issue lawyers always contemplate when it comes to global governance; we have fragmented regulation, and therefore foreign shopping. Companies can to some extent choose the jurisdiction. For example, Facebook is located in Ireland as far as data protection is concerned and the German Data Protection Officers do not really like that, but that's the EU.

Data protection as governance

Data protection online can be seen as part of the Internet governance structure. I would like to introduce our concept of governance. In our research we believe in a kind of rephrased Lawrence Lessig approach:

Many of you might know that our famous colleague from the United States has invented a kind of four-sector model when it comes to Internet governance, and his claim is that we shouldn't only look at state-set laws when we talk about the normative structure of the Internet and privacy and other issues, because social laws play a major role. Contracts play a role – there are contracts, e.g. between Facebook and the user. And of course "code," the hardware and software structure of the Internet, plays a major role. We have to consider the interplay of all those things to get the whole picture. That is our starting point when we do research on things like that and we believe that privacy governance has to be analysed along the same lines.

The global perspective

Finally I would like to address the global perspective on privacy governance. Frank La Rue was really to the point in his report made on behalf of the UNESCO in June 2013, when he noted that – focused on the state-citizen relationship – a main problem is still the lack of rules protecting privacy. He wrote: "Freedom of expression cannot be ensured without respect to privacy in communications" and that "National laws regulating what constitutes the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or simply do not exist."

It would be wise to address that, and one way of doing it is to look into ways of international harmonisation. One could say that this approach – suggested by the governments of Brazil and Germany after the NSA revelations – does not look very promising. However, if we look at the work of Mr. Greenleaf, who did a lot of comparative work on privacy issues, the picture brightens up considerably. He says that, especially due to EU regulation, a lot of thinking about data protection framework, harmonisation, etc. has started in many countries. The EU has coined the concept of the "third country," and by regulating the transfer of data to non-EU countries, to some extent it exports its data protection standards.

The EU Data Protection Directive (to be replaced by the General Data Protection Regulation) defines "third countries" as countries with no adequate level of [data] protection, unless they offer:

- Safe harbour,
- Binding/model/standard contractual clauses,
- Binding corporate rules.

It is one line of approaching global privacy governance to think about harmonisation of this kind. The draft General Data Protection Regulation discussed in Europe right now might have a similar effect, or even more intense effect, when it comes to international harmonisation.

Another aspect which might be interesting to consider tackling, for example, the NSA problem, is some kind of minimum standard, not complete harmonisation but minimum requirements. There is a lot of work we can build on when it comes to minimum standards, things I believe have not been at the centre of attention but should have been. One is the Granada Carta, by the International Working Group on Data Protection in Telecommunications

(IWGDPT) which already provides a minimum regulation, a set of rules that could be applied on an international level. Some countries – I already mentioned Brazil and Germany – have steered up a discussion about an additional protocol to an already existing international body of rules (Protocol to the International Covenant on Civil and Political Rights, 1966), especially dealing with minimum standards.

Also, at the next upcoming General Assembly at the UNESCO this topic will be discussed – as far as I have heard, the US and the UK have not really been backing this, not to say that they will try to hinder what would be the topic of the next general assembly, but there will be debate, definitely.

As for me there is a kind of state regulation failure when we address the problems I mentioned. National states do not really have an interest in limiting their own access to information. We can see that it is not only the US and the UK, other countries which are not in the limelight profit from privacy infringement by the NSA as well. Therefore, other stakeholders will have to raise their voices in the process of international standard setting.

Another line of approach focuses on the "code." Colleagues in Brazil actually think – like other software engineers – about re-engineering the Internet infrastructure in a way that it has a more decentralised user-centric approach: "If I personally have access to my data, when I give the key just to my doctor, I do not transfer my data to the global data base." Their argument – I'm just borrowing it and I bring it to you – is that the Internet infrastructure at present is more like a Big Data base, it is not user-centric, is has a more central approach, and that of course creates privacy disadvantages; so maybe we can think more alongside those lines.

As regards social norms, I believe autonomy is the key concept and I would like to explore this. A lot of research is needed there I believe; some is done here during this conference. We can see what autonomy means in an intercultural context.

As regards contracts, I believe there is a potential for transnational self- and co-regulation within the industry, based on contracts to make this system work.

Summing up, global privacy governance is indeed a complex endeavour; however, there is already substantial knowledge to build on where there is the will to optimise the structure.

Prof. Wolfgang Schulz, *Director at the Institute Humboldt HIG Berlin*. *Born in 1963, he studied law and journalism in Hamburg. Since 1997 he has been a lecturer within the field of information and communication at the law faculty of the University of Hamburg. In July 2009 he made his habilitation at the law faculty of the University of Hamburg through the Venia Legendi for public law, media law and law philosophy. Since July 2001 Prof. Schulz has been a member of the directorate of the Hans-Bredow*

Insitute. The focus of his work is on issues regarding the regulation of media content (specifically the portrayal of violence), issues regarding the regulation of new media (especially exposure of violence), questions concerning the legal basis of new communication media (specifically digital television and legal issues of journalism) as well as questions tackling a legal basis of the freedom of communication and descriptions of jounalistic systems according to systems theory. He also works on legal instruments of the state, for instance with regards to "regulated self-regulation." Wolfgang Schulz is an expert member of the parliamentary Enquete-Commission "Internet and digital Society" as well as a member of the committee of experts "Communication and Information" and of the advisory board "Diversity of Cultural Forms of Expression" of the German UNESCO Commission. Furthermore, he is a member of the Editorial Committee of the Journal of Media Law.

Legal Challenges Facing Global Privacy Governance

Claire Levallois-Barth

On 24 September 2013, the 35th International Conference of Data Protection and Privacy Commissioners observed that "there is a pressing need for a binding international agreement on data protection that safeguards human rights by protecting privacy, personal data" and resolved to call upon governments to advocate the adoption of an additional protocol to the United Nations International Covenant in Civil and Political Rights.[1]

However, since the 1980s, several legal data protection agreements have been adopted by international organisations:

- On 23 September 1980, the **Organisation for Economic Co-operation and Development** (OECD) published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[2]

- Fourth months later, on 28 January 1981, the **Council of Europe** adopted the so-called Convention 108 which still remains the only binding international legal instrument.[3]

- Then, in the mid-1990s, the **European Union** adopted its General Data Protection Directive.[4]

[1] 35th International Conference of Data Protection and Privacy Commissioners: A Compass in Turbulent World, Warsaw 23-26 September 2013: Resolution on anchoring data protection and the protection of privacy in international law, 24 September 2013.

[2] OECD, Recommendation of the Council concerning Guidelines Governing the protection of Privacy and Transborder Flows of Personal Data, 23 september 1980.

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

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 of 23.11.1995.

• Since 2005, the Asia-Pacific Economic Cooperation (APEC) has also its specific Privacy Framework.[5]

Despite different legal cultures and regimes, these texts make appear a consensus on the way to protect personal data (§1). This consensus, far from being challenged, is currently reaffirmed and reinforced in all the international instances (§2).

1. Consensus despite a difference of approaches

Broadly speaking, the study of the four major agreements underlines the growing consensus about the core personal data protection principles around the world (§1.1.), even if disparities in the conception of privacy can be noticed (§1.2.).

1.1. Commonly accepted core principles in international legal texts

The OECD Guidelines, which represent political commitments by the OECD's 34 member countries, and the Council of Europe Convention 108 ratified by 46 member parties embody the same principles of protection with many similarities. Mainly, the principles are:

– **Collection limitation:** There should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

– **Data quality:** Personal data should be relevant to the purposes for which they are to be used. To the extent necessary for those purposes, data should be accurate, complete and kept up-to-date.

– **Purpose specification:** The purpose for which personal data are collected should be specified no later than at the time of data collection. The subsequent use must be limited to the fulfilment of those purposes.

– **Use limitation:** Personal data should not be disclosed or made available for purposes other than those specified in accordance with the purpose limitation principle, except with the consent of the data subject or by the authority of law.

– **Openness:** Data controllers should provide clear and easily read statements about practices and policies with respect to personal data.

– **Individual participation:** An individual should have the right of access to and of correction of his personal data.

However, privacy principles provided in the 1980s are not identical in substance. Some divergences are significant. Convention 108 protects special categories of data, i.e. sensitive data that are more likely than others to

[5] APEC Privacy Principles, December 2005.

give rise to arbitrary discrimination, such as racial origin, sex life or political opinions. It also provides additional safeguards for individuals and requires countries to establish appropriate sanctions and remedies.

At the European level, if the data protection directive embodied a set of principles consistent with the OECD and Council of Europe agreements, the principles are somewhat stronger. The directive includes *inter alias* the establishment of Data Protection Authorities and a right to have disputes heard by the courts. It also requires to provide "opt-out" options for direct marketing uses of personal data as well as limitation on data exports to countries outside the EU which do not have an "adequate" level of personal data protection. So as to better align Convention 108 with the EU Directive, the Convention has been completed in 2001 by an additional protocol regarding the role of independent supervisory authorities and requiring data export limitations.[6]

Regarding the APEC Privacy Framework, this Framework promotes a weak standard from the European point of view, in that sense that principles present in other international instruments or in national laws of many countries, among which are the 21 APEC's members, are not reproduced. Thus, "the Principles in APEC's Privacy Framework are at best an approximation of what was regarded as acceptable information privacy principles twenty years ago when the OECD Guidelines were developed."[7] For instance, the APEC Privacy Framework does not limit collection to lawful purposes,[8] nor does it include the purpose specification principle. Moreover, new principles have appeared, testimony of the influence of the United States: The principles of "preventing harm" and of "choice" are ambiguous as to their effect and are capable of a vast number of interpretations and implementations. We also notice a complete absence of any obligations to enforce the principles by law. However, the APEC processes "have stimulated regular discussion of data privacy issues between the governments in the region and more systematic cooperation between Data Protection Authorities in cross-border enforcement."[9]

[6] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Strasbourg, 8.11.2001.

[7] Greenleaf, G., "Asia-Pacific developments in information privacy law and its interpretation", University of New South Wales Faculty of Law Research Series 5 (19 January 2007), p. 8.

[8] De Terwangne, C., "Is a Global Data Protection Regulatory Model Possible?", in *Reinventing Data Protection?*, Gutwirth, S.; Poullet, Y.; Hert, P.; Terwangne, C.; Nouwt, S. (eds.), 2009, p. 184. Also Pounder D.C., "Why the APEC Privacy Framework is unlikely to protection privacy?", http://www.out-law.com/page-8550.

[9] Greenleaf, G., "The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108", Edinburgh School of Law Research Paper Series, n° 2012/12, p. 17.

International agreements concerning data privacy have contributed a great deal to the development of consistency of national laws. According to Graham Greenleaf, in 2012, there were "81 countries providing comprehensive coverage of both their private and public sectors."[10] If enactment of laws outside Europe is accelerating, Graham Greenleaf's study demonstrates that the "European Standards" have influence outside Europe and that this influence increases.

1.2. Disparities in the conception of privacy

Generally speaking, the APEC Privacy Framework considers privacy under the economic angle, as a consumer matter. This is also the OECD and EU-US Safe Harbour agreement approach. Following this angle, three personal data are marketable goods. Their protection has to be "balanced with private interest."[11] The US, for instance, hardly accepts imposing "burdens" on economic activities in the name of data protection. "This leads to no real rights being guaranteed to the data subject: Individual access to one's personal information may be refused when there is an overriding private interest or when the burden it would lead to would be disproportionate to the risks."[12]

On the other hand, privacy can been seem as a fundamental right. This is clearly the Council of Europe's and the European Union's approach. In fact, there are two different human rights but complementary rights:

- **The right to privacy** is firmly established by law *inter alias* in article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR) of the United Nations, in article 12 of the 1948 Universal Declaration of Human Rights, and in article 8 of the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms of 1950.
- **The right to the protection of personal data** is more recent: It is recognised by the 2000 EU Charter of Fundamental Rights, which has endorsed the fundamental role of independent Data Protection Authorities. This right is promoted on an equal level with the right to privacy and freedom of expression.

At the national level, more and more Constitutions are amended with a separate right to data protection next to the more classical right to privacy. Generally, privacy protects the opacity of the individual by prohibitive measures (non-interference). It is associated with autonomy, dignity and trust. Its protection is indispensable to the protection of liberty and democratic institutions. Data protection by default calls for limitation and trans-

[10] Greenleaf, G., *op.cit.*, p. 3.

[11] De Terwangne, C., *op. cit.*, p. 181.

[12] De Terwangne, C., *op. cit.*, p. 181.

parency of the processor of personal data and gives the individual subjective rights to control the processing if his/her personal data.[13]

2. Movement of convergence of the international legal texts

If the convergence of the international texts through their revision represents a way to achieve privacy protection (§2.1.), this solution has to be combined with approaches aiming at producing more international legal harmonisation (§2.2.).

2.1. Revision of the existing texts aiming at more effectiveness

The OECD Guidelines were up-date in 2013.[14] The newly revised Guidelines take place in a general international movement of coherence of international legal texts. Today Convention 108 is being revised, while the EU discusses a new draft data protection regulation on the matter.[15] These reviews all point in the same direction: The core principles have proved to be capable of adapting to the evolution of technology and reality, and there is an increased focus on implementation and enforcement. The key word is really "more effective protection in practice." For instance, newly OECD Guidelines strongly put emphasis on the accountability of responsible organisations: An organisation's data controller must have a data "privacy management program" and be prepared to demonstrate it is appropriate at the request of a privacy enforcement authority.

The new Guidelines introduce the concept of a "privacy risk assessment," echoing the "privacy impact assessment" required under the draft European Union data protection regulation. Newly OECD Guidelines insert of a data security breach notification: This US-originated concept covers both notice to an authority and notice to an individual affected by a security breach affecting his/her personal data. Contrary to the draft EU regulation, the OECD's Guidelines take a more risk-based approach by limiting the notification requirement to significant security breaches. OECD Guidelines also include a reference to "privacy enforcement authorities," which did not exist explicitly under the 1980 version, specifying they should have the "governance, resources and technical expertise necessary to exercise their powers

[13] De Hert, P. and Gutwirth, S., "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionlisation in Action", in *Reinventing Data Protection?*, Gutwirth, S.; Poullet, Y.; Hert, P.; Terwangne, C.; Nouwt, S. (eds.), 2009.

[14] OECD, Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as amended on 11 July 2013.

[15] 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, 25.01.2012.

effectively and to make decisions on an objective, impartial and consistent basis."

However, the OECD Guidelines do not include language on a "right to forget" or on "Privacy-by-design," concepts that are in the draft EU data protection regulation.

2.2. Approaches aiming at producing more international legal harmonisation

One option is to draft a new Convention. In recent years, a number of influential entities in both public and private sectors have called for this solution. Some companies have made such an appeal, as Goole did in 2007, calling for the creation of "Global Privacy Standards." The International Conference of Data Protection and Privacy Commissioners has also called for a universal international instrument for several times.

At the United Nations level, protection of personal data is presently on the long-term programme of the International Law Commission. Mainly, the drafting of any such convention would take a minimum of ten year, if at all. There is no doubt that an international convention can produce a greater degree of harmonisation, since it results in a single text that is legally binding on states that enact it. However, such binding nature can make states reluctant to do so. A Convention can also be subject to reservations made by states.[16]

Another option would be to have states accede to **Convention 108**. This is possible because the Council of Europe has opened accession to the Convention to all countries. However, accession by non-member states of the Council of Europe is only open to those with data protection legislation that have an appropriate level of protection. For different legal reason, it can hardly create binding rights on behalf of individuals since individual rights cannot be derived from a Convention which is not self-executing. In others words, Convention 108 may only be enforced against a Council of Europe non-member country before the European Court of Human Rights if this country has acceded to the European Convention of Human Rights.

Another way to produce international harmonisation is through instruments of recognition of foreign data protection standards. This kind of system is foreseen in the **adequacy principle** developed in the EU directive and the proposed Data Protection Regulation. The adequacy principle is a functional concept in order to allow meaningful data exchange with countries outside the EU: This exchange is subject to adequate protection of personal data, but not necessarily to a fully equivalent protection, e.i. with the level of protection

[16] Kuner, C., "An international legal framework for data protection: Issues and prospects", *Computer Law & Security Review* (2009) 307-317.

within the EU. The first requirement covers certain key data protection principles that should be embodied in the third country's framework. The second requirement looks at available mechanisms to deliver a good level of compliance, to provide support to individual data subjects and to provide appropriate redress to injured parties where rules have not been complied with. Even if the list of adequacy decisions is not impressive; however, it is growing: Israel, Uruguay and New Zealand were added recently. It is also likely that the list will grow in the future. The draft regulation has provided for more flexibility by allowing adequacy decisions for a territory or a processing sector within a third country, and by introducing the possibility of finding an adequacy for an international organisation.

Finally, the growing practice of **cooperation among data protection authorities** both in Europe and on other continents can give considerable weight to more global privacy practices. Since 2010, the Global Privacy Enforcement Network (GPEN) has grown to include members from Europe, Asia, North American and the Pacific. The US Federal Trade Commission is playing a very active role and is working together with supervisory authorities in Europe, Canada and other APEC countries.

Since most data protection legislations are based on the same international documents, the fundamental principles of law are similar across regions and legal system. However, the differences in the cultural, historical and legal approaches to data protection and privacy mean that once one accesses to the highest level of abstraction, there can be significant differences. I do not think we will end-up with full harmonisation across the globe. A certain degree of diversity will always remain. It is unavoidable and even desirable.

Claire Levallois-Barth *is doctor in law, Maître de conférence at the Economic and Social Science Department at Télécom Paristech. She specialises in new technologies law, especially in privacy and data protection law both at the French and international level. Her studies are related to the application of these legal aspects to new technologies such as location-based services, Bluetooth and social networks. She is the coordinator of the Chair "Valeurs et Politiques des Informations Personnelles" (Institut Mines-Télécom). She is the general secretary of the French Association of Personal Data Protection Officials (Association Française des Correspondants à la Protection des Données à Caractère Personnel - AFCDP) and she is a Data Protection Official.*

Global Privacy Governance: A Comparison of Regulatory Models in the US and Europe, and the Emergence of Accountability as a Global Norm

Winston J. Maxwell

In the field of global privacy governance, we often hear of the tension between the European and US models. The clearest manifestation of this tension is the fact that the United States has not been found to provide "adequate" protection for personal data by the European Commission. Transfers of personal data to the United States are therefore tightly controlled.[1] Yet the United States and Europe have more in common than most people think. Both regimes are based on FIPPS, Fair Information Privacy Practices reflected in the 1980 OECD Guidelines. In spite of some philosophical differences, Europe and the United States can end up with similar practical solutions, such as for mobile apps. Importantly, both Europe and the United States are emphasizing co-regulation and "accountability" as regulatory models. APEC's Cross Border Privacy Rules also emphasise accountability, making accountability the emerging theme for global privacy governance.

The United States and Europe share a common data protection heritage

Privacy protection in the United States has its earliest roots in the Fourth Amendment of the US constitution. Prior to US independence, British soldiers routinely burst into the homes of citizens, which prompted the drafters of the US constitution to include a fundamental right to protection of the security of each individual's home against government intrusion. The Fourth Amendment is focused on intrusions by the government, not by private

[1] Transfers are prohibited unless one of the exceptions applies: safe harbor, standard contractual clauses, binding corporate rules, etc.

actors. Although originally focused on the individual's home, the Fourth Amendment has been extended to other contexts where individuals have a reasonable expectation of privacy similar to what they would enjoy in their own home. For example, the Supreme Court recently held that the placing of a GPS tracking device on the outside of a car was the equivalent to a search of an individual's home which should have a search warrant. Another decision held that the use of police dogs to sniff around the outside of a home constituted a virtual search of the home, again requiring a search warrant. Wiretaps and certain other forms of electronic surveillance are also covered by the Fourth Amendment.

Because of sensitivity in the United States against privacy intrusions by the government, the United States enacted in 1974 a general law protecting individuals' personal data in the hands of the government. The Privacy Act of 1974 embodied the concept of FIPPs (Fair Information Privacy Practices) that originally were introduced in a report by the US Department of Health Education and Welfare. FIPPs later became the basis for the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which themselves formed the basis for the 1995 European Data Protection Directive.

In the late 19th century, US legal scholars began to recognise the need for privacy protection not only against the government, but against private parties who unreasonably invaded another person's private space. The much-cited Warren and Brandeis article, "The Right to Privacy,"[2] was prompted by the publication of photos in newspapers showing people in unflattering situations. The Warren and Brandeis article led to development of common law torts of privacy that protect various aspects of an individual's personal life and image. At about the same time as the Warren and Brandeis article, there were lawsuits in France dealing with the publication of unflattering photos in newspapers, which led to the enactment of a law in France, limiting publication of photos without an individual's consent.[3] Today, Article 9 of the French Civil Code recognises each person's right to his or her private life and image. This is similar to the four "privacy torts" defined by William Prosser in the US: (1) intrusion upon seclusion; (2) public disclosure of embarrassing private facts; (3) false light publicity; and (4) appropriation of name or likeness.[4]

In addition to the privacy torts, which are matters of state law, the United States has developed a series of statute-based laws dealing with personal

[2] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev., 1890. 193.

[3] French press law of June 4, 1868.

[4] William L. Prosser, *Privacy*, 48 Calif. L. Rev., 1960. 383, 383.

data in certain sectors. At the federal level, eight different privacy laws exist, each with a different acronym and scope of application:

- HIPAA (Health Insurance Portability and Accountability Act) – health data,
- GLBA (Gramm-Leach-Bliley Act) – financial data,
- COPPA (Children's Online Privacy Protection Act),
- FCRA (Fair Credit Reporting Act),[5]
- ECPA (Electronic Communications Privacy Act),
- VPPA (Video privacy protection act),
- Cable TV Privacy Act,
- "Can-SPAM" Act.

Some of these laws are at least as restrictive as European data protection laws, although their scope is more limited. In addition to these focused federal laws, there exists a myriad of state laws dealing with targeted privacy issues. The State of California is particularly active, having enacted laws targeting the collection of data via the Internet as well as the so-called "eraser" law, which permits minors to delete their personal data on Internet platforms.[6] California also has a general right of privacy included in the state's constitution. Almost all states in the United States have laws regulating how data breaches should be notified.

In addition to these focused statutes, the United States has a general statute on consumer protection that has been used extensively as a means to protect personal data. Section 5 of the Federal Trade Commission Act prohibits any unfair or deceptive practice and empowers the Federal Trade Commission (FTC) to enforce the provision against companies. Over recent years, the Federal Trade Commission has proactively expanded the concept of unfair and deceptive practice to include processing of personal data by companies in ways that do not match the reasonable expectations of consumers. The FTC's first point of focus is on the privacy policies that companies themselves publish. If any of the statements in the privacy policy are not respected by the company, either in spirit or in letter, the FTC will accuse the company of an unfair and deceptive practice. The FTC has expanded the concept of unfair and deceptive practice to cover information security, thereby putting a relatively high burden on companies to take measures to protect personal data against unauthorised disclosure. The FTC has a wide range of tools at its disposal, going from soft measures such as workshops and guidelines to more draconian measures such as sanctions and, importantly, settlement agreements. (We will return to the subject of settlement agreements in the second part of this article.)

[5] Incidentally the FCRA includes a form of "right to be forgotten."

[6] For a description of California's privacy laws, see, http://oag.ca.gov/privacy/privacy-laws.

The FTC uses these tools to send signals to the market regarding the FTC's interpretation of the vague "unfair and deceptive" standard. Professor Solove refers to the FTC's "new common law of privacy."[7] Many states have their own authorities (generally the attorney general), which enforce state privacy rules. Those state authorities can issue guidelines in addition to those of the FTC. The recent guidelines issued by the California Attorney General on mobile applications[8] contain recommendations that resemble in many respects the position of Europe's Article 29 Working Party.[9]

Even in matters involving government surveillance, US and European laws are not as far apart as they might seem. Like most European countries, the United States has a separate set of rules for normal police investigations and for national security operations.[10] Police investigations are governed by the "Crimes and Criminal Procedure"[11] section of the US Code, whereas national security investigations are governed by the "Foreign Intelligence Surveillance" and "War and National Defense"[12] sections of the Code. This is similar to the legal structure in France: the *Code de procédure pénale* governs surveillance in the context of criminal investigations, and the Code de la sécurité intérieure governs surveillance in the context of national security. As can be expected, the rules surrounding national security provide fewer safeguards and less transparency than the rules applicable to criminal investigations. In criminal investigations, police must obtain a court order before conducting intrusive surveillance. In national security matters, authorisations may be given by a separate national security court (in the US) or by a specially named person in the Prime Minister's office (in France).

The Snowden affair has raised serious questions about the adequacy of the US framework for national security surveillance. A recent report commissioned by President Obama shows that the US regime for collection of data in national security cases requires improvement, in particular to better protect privacy of both US and non-US citizens.[13] The European Commission also listed areas where the US could help restore trust in cross-border data flows, including the

[7] Daniel Solove and Woodrow Hartzog, "The FTC's New Common Law of Privacy", August, 2013, www.ssrn.com.

[8] California Attorney General, "Privacy on the Go, Recommendations for the Mobile Ecosystem", January 2013 http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[9] Article 29 Working Party, Opinion n° 02/2013 on apps on smart devices, WP 202, February 27, 2013.

[10] Winston Maxwell and Christopher Wolf, "A Global Reality: Governmental Access to Data in the Cloud", Hogan Lovells White Paper, May 2012.

[11] Title 18, US Code, "Crime and Criminal Procedure."

[12] Title 50, US Code, "War and National Defense."

[13] "Liberty and Security in a Changing World", Report and Recommendations of the President's Review Group on Intelligence and Communications Technology, Dec. 12, 2013.

negotiation of an "umbrella agreement" with Europe regarding government surveillance.[14] The Snowden affair has also shown that the United States is not alone: intelligence agencies in major European countries conduct similar data collection practices with little or no court supervision.[15] The debate is therefore not "US versus Europe," but a more fundamental question of finding the appropriate balance between security and privacy in a data-centric age. Both security and privacy are fundamental rights. Without security, privacy cannot exist – security is an "enabler" of other fundamental rights.[16] By the same token, security cannot swallow privacy. Finding the right balance is not easy, and new data gathering techniques give these questions a new dimension and urgency. The Snowden affair has had the merit of bringing the issue to the forefront so that those debates can occur before national parliaments and courts.

We have seen a number of similarities between Europe and the United States, as well as common issues relating to government surveillance and fundamental rights. What are the main differences between the two frameworks? The differences have been examined in detail elsewhere.[17] Suffice it to say here that one of the key differences is philosophical: In the United States, certain areas of personal data are surrounded by strict safeguards (eg. HIPPA, GLBA). However, outside of those closely regulated areas, companies are free to exploit data as long as they do not commit an unfair consumer practice. In Europe, personal data is attached to a fundamental right. The starting point for analysis is that any exploitation of data potentially violates a fundamental right and must therefore have a compelling justification. Some data (eg. sensitive data) require a high level of justification, other data require less. But the starting point is that each individual has a personal right to control his or her personal data, and that processing by others is forbidden unless justified by a list of well-defined reasons. In practice, the US and European approaches often lead to the same practical result, but the reasoning begins from different points.

The US and Europe converge in co-regulation and accountability

Co-regulation is a system under which a state-sponsored institution, such as a government agency or independent regulatory authority, creates a frame-

[14] European Commission Press Release: "European Commission calls on the US to restore trust in EU-US data flows", November 27, 2013, IP/13/1166.

[15] See, e.g., Jacques Follorou and Franck Johannès, "*Révélations sur le Big Brother français*", *Le Monde*, July 5, 2013; Winston Maxwell, "Systematic government access to private-sector data in France", International Data Privacy Law 2014, Oxford, forthcoming.

[16] In France, this principle was affirmed by the Constitutional Council in decision n° 94-352 DC of January 18, 1995 in connection with videosurveillance.

[17] Christopher Wolf and Winston Maxwell, "So Close, Yet so far Apart: The EU and US Visions of a New Privacy Framework", *Antitrust*, Vol. 26, no 3, 2012.

work within which private actors discuss and if possible agree on regulatory measures. Co-regulation is like self-regulation, except that in co-regulation the government or regulatory authority has some influence over how the rules are developed, and/or how they are enforced. This is supposed to make the rulemaking process more legitimate and effective compared to purely self-regulatory solutions. It is more legitimate because the process is supervised by officials who are accountable to the democratically-elected legislature. It is more effective because the resources of the state can be used to enforce the rules.

Data protection authorities in Europe are distrustful of purely self-regulatory arrangements, and prefer co-regulatory solutions in which the data protection authority (DPA) is involved in both the formation of rules and their enforcement. DPAs in Europe emphasise binding corporate rules (BCRs), which evidences this co-regulatory preference.

Under the European data protection directive, companies are prohibited from sending personal data outside the EEA to countries that have not been recognised by the European Commission as providing an adequate level of data protection. The United States currently is not viewed as providing an adequate level of protection of personal data. One of the ways companies can overcome the prohibition is by adopting BCRs. BCRs are a set of internal procedures that guarantee a high level of protection of personal data throughout the organisation, including in parts of the organisation located in countries without "adequate" protection. BCRs must be developed in close cooperation with DPAs in Europe. A multinational group can propose BCRs following a template adopted by the Article 29 Working Party, but ultimately the content of the BCRs must be negotiated point by point with one of Europe's DPAs. Once the lead authority is satisfied with the content of the BCRs, the file is then sent to two other co-lead DPAs who in turn scrutinise the content of the file to ensure that the BCRs meet European standards. Once the BCRs have been approved, they confer rights on third parties who can sue the company for any violation of the BCRs. Likewise, any breach of the BCRs can give rise to sanctions by DPAs.

BCRs constitute co-regulations because they are developed by private stakeholders within a framework established by regulatory authorities, and once they have been adopted, the BCRs can be enforced by regulatory authorities in the same way as classic regulations.

The Federal Trade Commission's (FTC) extensive reliance on negotiated settlement agreements can also be seen as a form of co-regulation. The FTC conducts investigations and begins enforcement action against companies that have violated the "unfair and deceptive practices" rule, as well as other privacy violations such as violation of the US-EU safe harbor framework. One of the procedural options that the FTC can propose is a settlement agreement with the company, which binds the company to put an end to the relevant practices as well as submit itself to on-going accountability obligations similar to those one sees in BCRs.

The individual settlement agreements provide for procedural and structural safeguards to help prevent violations of data privacy commitments.[18] Like European BCRs, the negotiated settlement agreements provide for both internal and external audit procedures, training programs and periodic reporting to the FTC. The settlement agreements last for 20 years, giving the FTC the ability to co-regulate major Internet companies over a long period of time. The FTC settlement agreements are public, thereby permitting the FTC to use the settlement agreements as a means of sending signals to all companies in the relevant sector. Although the settlement agreements are not binding on companies that are not signatories, the settlement agreements provide to third parties guidance on what the FTC considers to be the state of the art in terms of privacy compliance. The settlement agreements inform third parties on practices that the FTC is likely to view as unacceptable, as well as compliance measures that the FTC is likely to consider as optimal.

The FTC settlement agreements can have wide ranging effects. First, if the settlement agreement binds a major Internet platform such as Facebook, the settlement agreement will have an impact on a large portion of the Internet industry simply because the platform represents a large part of Internet users. Second, the settlement agreement will have indirect effects on all other players in the Internet industry, by showing best practices and FTC expectations. The FTC's settlement agreements serve a pedagogical function, thereby contributing to overall compliance with regulatory best practices in the industry.

The United States government is trying to encourage other co-regulatory solutions for data privacy. The US administration refers to this as the "multi-stakeholder process." Under the multi-stakeholder process, the National Telecommunications and Information Agency, the NTIA, convenes stakeholders in an effort to develop codes of conduct. The role of the NTIA is to organise multi-stakeholder meetings, facilitate the exchange of information, and apply the threat of mandatory regulatory measures should the stakeholders fail to agree on consensual measures. The NTIA acts as a maieutic regulator,[19] helping to nudge stakeholders toward a consensus. The presence

[18] For an example, see the Facebook settlement agreement here: http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[19] Nicolas Curien, "Innovation and Regulation serving the digital Revolution", *The Journal of Regulation*, 2011, I-1.32, p. 572-578.

of the government in the discussion also ensures that the self-regulatory measures that emerge from the discussions satisfy public interest objectives, and in particular, the protection of privacy rights. The multi-stakeholder process recently yielded draft recommendations on transparency in mobile applications.[20]

The emphasis on co-regulation is not surprising given the emphasis on accountability in the 2013 OECD Guidelines, the proposed European Data Protection Regulation, the APEC Privacy Framework and in the White House's Consumer Privacy Bill of Rights.[21] Accountability amounts to internal privacy compliance programs implemented by companies that then create legally binding rights and obligations – a form of co-regulation.

The convergence of US and EU co-regulatory philosophies will be tested in connection with efforts to create a compatibility system between European BCRs and Cross Border Privacy Rules (CBPR) developed under the APEC framework.[22] Like BCRs, CBPRs represent a set of data protection obligations that companies can subscribe to, and that will be enforced by data protection authorities in participating APEC countries. Application of the rules is verified by an "accountability agent."[23] The purpose of subscribing to the CBPRs is to demonstrate compliance with the APEC Privacy Framework principles,[24] and thereby facilitate data flows among APEC economies. An international group that successfully implements both BCRs and CBPRs would meet accountability obligations under both EU and APEC frameworks. Accountability is therefore becoming the pillar of an emerging global privacy governance model.

Winston Maxwell *is a partner with the international law firm Hogan Lovells, and is recognised as one of the leading media, communications and data protection lawyers in France. Winston Maxwell is a co-author of* La Neutralité d'Internet *(La Découverte, 2011) as well as numerous articles on Net neutrality, data protection law, and telecommunications regulatory issues. Winston Maxwell teaches courses on data protection and regulation of the digital economy at Télécom Paristech and HEC in France, and advises both regulators and corporate clients on Internet, data protection, media and telecom regulatory matters. He received his law degree in 1985 from Cornell Law School and is admitted to practice law before both the Paris and New York bars.*

[20] http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[21] United States White House, "Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy", February 2012.

[22] http://www.apec.org/Press/News-Releases/2013/0306_data.aspx.

[23] For a full description of CBPRs, see http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

[24] http://publications.apec.org/publication-detail.php?pub_id=390.

The CNIL and Global Privacy Governance[1]

Florence Raynal

Introduction

Global privacy governance is at stake because data privacy has become a growing issue at a worldwide level for citizens, governments and business.

Personal data are necessary for almost all business and public services, they do not know geographical borders anymore and are an essential element of the future of the Internet economy.

There are strong expectations from our citizens to get a robust and effective protection for their right to privacy wherever their data are handled. They claim guarantees to trust business operators and public institutions about the way they respect their privacy.

Companies are more and more integrating privacy as part of their business strategy and as an element of competiveness to make the difference and develop clients' confidence.

Regulators, legislators, governments are reforming fundamental texts such as the OECD privacy guidelines, the Convention 108 or the EU Directive 1995, or creating new approach (e.g. APEC privacy framework).

Those historical revolutions coming in will have a direct effect on global privacy governance and will shape our regulatory environment for data privacy.

The CNIL has been actively involved in following the debates around those reforms promoting a European approach on privacy matters and in developing European and International cooperation among data protection authorities, which is a key element of global privacy governance.

[1] Transcription of the speech given during the Privacy seminar of Institut Mines-Télécom.

Upcoming changes impacting global governance

EU

The EU has been reviewing its framework since 2010 with the reform of the EU directive 1995. The Council is currently discussing their amendments to the text proposed by the EU commission in 2011 and the Committee on Civil Liberties Justice and Home Affairs of the European Parliament voted on their own amendments on October 21st 2013.

The CNIL is in favor of the text proposed by the EU Commission, which creates a new way to approach privacy. In a nutshell, the proposed text:

– Reinforces the rights of the data subject (e.g. more transparency, right to be forgotten, right to portability);

– Creates a new balance, shift in paradigm with a simplification of the filing requirements with Data Protection Authorities and the introduction of a concept of accountability for controllers and processors. Accountability is an additional principle, framed by law, to comply but also to demonstrate effective compliance. This offers a chance for better, real and effective protection and for framed co-regulation;

– Introduces notification of security breach for all sectors and a legal framework for processors;

– Offers harmonization of powers and competences between Data Protection Authorities (including sanctions);

– Confirms the application of European Union law to foreign data controllers if EU citizens are targeted;

– Last but not least: Keeps the fundamental values (e.g. legitimacy, proportionality, retention, information, rights of the data subjects).

Still, we have some concerns, in particular about one proposition of the EU Commission creating a one-stop-shop based on the main establishment of the company for pan-European data processing. In other word, the business will be able to choose its competent Data Protection Authority. This could create forum shopping and diminish the protection for data subjects, limiting the ability of national Data Protection Authority to protect them effectively and imposing the citizen to exercise their recourse action before a foreign court.

OECD

The OECD just adopted on July 2013 its new privacy guidelines. We all know that those guidelines do not have any legal value as such, but they represent a strong political message as 34 governments of the EU but also of the APEC (US, Canada, Japan) are adopting them. They represent a standard, an orientation that governments should follow locally.

The new rules put an emphasis on the accountability concept but also push for the designation of data protection authorities in the world and underline the need for better international cooperation and interoperability.

As the European Union is in the process of changing its privacy framework, it is essential to follow with great care these evolutions and maintain the "*acquis communautaire*."

Council of Europe

The same is happening at the Council of Europe with the modernization of the Convention 108 that is on its way and that should be adopted in 2014.

This text, which is the first European binding instrument of data protection, bounds 45 members (over 47) and has the legal value of a Treaty.

Therefore, changes made on this convention are key for the European Union and will have a direct impact on our regulatory framework.

Asia and the US

There is a strong implication of the US and of Asia that is very much linked to the necessity to create trust on the Internet. Privacy becomes a key element for the development of the Internet and economic growth.

There is one initiative to stress out, called the APEC cross-border privacy rules (CBPR). The APEC is composed of 21 members, among them the US, Russia, China, Singapore, Japan and Canada. The CBPR have been developed by APEC to guarantee a free flow of information within the APEC zone.

The CBPR are very close to one EU instrument for transfers of personal data, called Binding Corporate Rules (BCR).

BCR is an interesting tool for global governance defining as a global privacy policy, the fundamental values on privacy of a multinational corporation but also covering the mechanisms to implement them within the group (such as audit, training programs, global network of privacy officers…). They are used to frame internal group transfers made from EU but also as a global internal compliance programme on privacy. Using BCR allows transferring EU data freely around the globe.

We have initiated an analysis of the APEC CBPR to compare them to our BCR and to see whether we could connect them.

In that regard, a committee APEC-EU has been set up and regularly meets. The WP29 and APEC are currently drafting together a common referential to provide the business established in both zones with some guidelines on how to satisfy both requirements and then to apply for double certification (EU and APEC).

French speaking network of Data Protection Authorities (AFAPDP)

The CNIL is also involved within the AFAPDP whose aim is to share experience, resources and information on data privacy. The AFAPDP members will decide at the next annual conference in November 2013 on the adoption of a new tool to frame international transfers of the French speaking zone based on the European BCR and called the RCE (Règles Contraignantes d'Entreprise). Their validation will be based on a strong cooperation among data protection authorities and will guarantee a high level of protection for data flows.

Conclusion

There is food for thought and lot of initiatives at the moment for building global privacy governance and the key word for data protection authorities is "cooperation" for example by creating "interoperability" among different regimes.

Trying to agree on common or adequate values and rules is not necessarily the Holy Grail, what is important is to create tools, bridges and paths to navigate between different ecosystems. It is exactly what the CNIL is trying to achieve with the APEC with a strong cooperation between the EU WP29 and the APEC data privacy working group or with the French speaking countries.

Indeed, we deeply believe that one of the corner stones is to improve cooperation between Data Protection Authorities at EU level but also at international level. A good example at EU level is the WP29 enforcement taskforce on the Google case. At international level, the international conference of privacy commissioners recently adopted a resolution calling for a strategic plan to refine the Conference and enhance its capacity for action. The idea is to define a new governance model and to develop a real and effective network at global level at international level for exchanging information, best practices and organizing joint enforcement actions.

I am not sure that we have today the solution for global privacy governance, but there is a need, a strong willingness from all stakeholders with that objective in mind. Ideas are on the table like stones. Now, let's build the house!

About the CNIL

The CNIL (Commission Nationale de l'Informatique et des Libertés) is the French Data Protection Authority mainly responsible for:

–Regulating data processing activities of business and public authorities (competent for both private and public sectors);

–Informing citizens on their rights for the protection of their personal data, advising controllers on their obligations;

–Investigating privacy practices and complaints;
–Sanctioning in case of violations;
– Anticipating the future, following IT developments to adapt our regulation and doctrine.

The main text of reference under French Law is the French Data Protection Act of 1978 modified in 2004 to implement the European Union (EU) Directive adopted in 1995.

The CNIL has 27 counterparts in the European Union and we are working closely together via the structured network of the Working Party 29 (WP29). We have regular meetings, working groups on key subjects (e.g. technologies, e-government, international transfers, police and justice, financial matters) and we adopt common opinions on shared issues.

At the international level, there are today around 80 "CNILs" in the world that meet once a year and issue common resolutions (such as on enforcement cooperation, digital education, profiling, web tracking...).

Florence Raynal, *Head of European and International Affairs of the CNIL. She started her career in 2000 in New York within the International Law Firm of Ernst & Young. Back to France in 2004 Florence Raynal advised multinationals on European privacy cross-border projects. She was also in charge of internal privacy compliance for Ernst&Young in the European Western area and was appointed Data Protection Officer (Correspondant Informatique et Libertés) for Ernst&Young France in 2007. She was then appointed at the CNIL in 2008, Head of European and International Affairs, in charge of defining and promoting CNIL's position on international and European matters.*

Privacy and Identity in the Digital Age[1]

Pierre-Emmanuel Struyven

Privacy can be described as the ability for individuals to disclose personal data in a controlled manner. It is a matter discussed by regulators, lawyers and consumer organisations alike. In today's digital world, Privacy and Identity are at the heart of many business models and consumer propositions. In this speech, I'll try to highlight how privacy and identity are at the core of digital lifestyle and business innovation for pure-player digital services but also legacy/brick-and-mortar business models.

Being anonymous in the digital era

Privacy is definitely not a black and white issue. There is a constant trade-off to disclose or not personal data and facts for the consumers; and also a trade-off for organisations to use or not these data. Absolute privacy would be anonymity, a perfectly valid choice in theory, but a challenge in the digital era where part or even most of my connected life leaves a trace in countless systems and databases, with countless private and public organisations. In theory I can use some services anonymously, but the service level is then somewhat limited. As soon as transactions or personalised services are involved I need to be identified and, therefore, my Identity will be linked to *explicit* personal data that I will voluntarily disclose, such as my age, my address, my preferences… The very use of a service will also provide a lot of *implicit* or *contextual* information about an individual: products purchased or browsed in a catalogue, websites visited, so-called social graph of people in their environment, physical locations visited, etc.

Using personal data allows businesses and organisations to deliver better service to their customers. It is even the root of many new business models, where on the one side individuals give information and on the other side they

[1] Transcription of the speech given during the Privacy seminar of Institut Mines-Télécom.

receive a free and relevant service. Search engines or targeted advertising are typical examples of such deals between users and the services they use. We know that storage and use of personal data is a highly regulated area. At the end of the day, the customer is the main judge: am I satisfied with the service I receive and am I happy about the way my personal data are used.

Physical and digital channels, multiple identities

Privacy is not a new topic that arises with Internet and online services. The regulation of privacy in France dates back to the first massive computer files and the technical ability to manipulate and cross them. With the Internet, the quantity of data, the number of parties involved changes magnitude. Access to personal data is also possible for virtually any organisation or person through the Net, where they are often available without restriction (e.g. birth date through profile in social network, phone number through phone directory). Therefore, the privacy challenge is not only a question about disclosing explicit or implicit data, but also of managing who it is disclosed to and how it is managed over time. Social networks illustrate this challenge perfectly: what information do I want to disclose, to whom, am I able to change it later, e.g. when I quit college and move into a professional career.

Social networks also raise the question of the aliases. I am one single person, but I may want several different identities (or profiles) online to manage my privacy: one for my family, one for my friends and one for my colleagues.

The challenge is not limited to the online sphere but circles between the online and the physical world. Your digital footprint, the information about you that you leave everywhere, is linked to what you do online but is also linked to what you do in the physical world. For instance, businesses are increasingly embracing the "omni channel" paradigm where sales channels are closely linked together. Typically if you consider buying a new TV set, you will start your product discovery on the Web, then you will go to the local shop knowing the product is stocked there, afterwards you will probably go back online to buy accessories and call customer care to get support about this new TV. To deliver the optimal experience, this merchant will encourage the visitor of his website to identify itself in order to keep track of his choice, reserve the chosen product at the local point of sale, etc.

The mobile acceleration

With mobile phones and tablets, we have increased our usage of digital services: more interactions every day and throughout the day, more businesses and services involved, more people having access – new geographies that discover mass Internet through mobile and also younger demographics that are connected 24/7.

We do everything digitally today: we check our mails online and increasingly on mobile phones, we check credit card balance and bank account with increasingly popular mobile banking applications, we use e-administration to check social benefits.

The mobile is also going to be used to pay at the counter (NFC based credit card payment) or to secure online payment (two-factor authentication), board public transports, and store loyalty cards. We really live *with and in* a digital world and we leave traces everywhere and all the time.

Many online and mobile services are free for the end user. It is the basic business model of search engines: through my query I tell the service what I'm looking for, therefore giving away a little piece of information about my interests, and in return I will get a fairly accurate result. Brands and corporations are ready to pay to be featured in the search results, because they are exposed to relevant customers in a relevant context. Similar two-sided business models are found in price comparison engines or social networks. Mobile or tablet usage is amplifying this already well-established model, because usage is fast developing on mobile and that using the actual localisation of the user creates new opportunities in targeting.

So there really is a win-win deal between consumers, trading personal information in return for service and relevance. It is a very important paradigm, when one speaks about privacy because it means that, as a consumer, I'm ready to trade some of my privacy in return for a service.

Not so different is the use of personal and usage data to improve the customer experience. Most e-commerce sites use it to maximise their performance by showing one customer the most relevant products: relevance by linking to existing purchase history or catalogue browsing, relevance by suggesting products that similar customers have purchased. Recommendation engines are increasingly important in many businesses selling physical goods or digital content. When browsing huge online catalogues – even more so when browsing happens on the go on the mobile or the TV screen – receiving relevant recommendations or seeing relevant product categories first not only enhances my experience as a user but also increases sales.

Targeted advertising is another example where being identified and exposing more or less explicitly personal data, changes the experience for the end user. Targeting is a major trend for digital marketing, Web and mobile ads. With online advertising, you can target your audience in a very detailed way, possibly down to the individual user. This was not possible in traditional *mass*-media such as TV. On one hand, again as a consumer, if I'm using a service where ads are displayed, I'd rather receive relevant ads than ads that are absolutely not interesting to me. But again on the other hand, it means that whoever is delivering the ad has identified me and has linked information about me to the identifier. It is likely that this happens completely within the ad-serving infrastructure (through the use of cookies, IP address, device id, etc.) and that the website publisher has nothing to do with it. But in the mind of the consumer, it is hard to tell if the targeted ads are the result of the Web publisher giving access to some of my personal data or if it is done by using technologies such as cookies.

Targeted ads can go one step further now with localisation. Using the GPS embedded in smartphones, using the cellular or Wi-Fi network, it is possible to know where a mobile or a tablet is located. Using localisation for targeting requires the user consent (opt-in). A user who has opted-in for such a service will receive information from brands offering rebates or promotions when it enters a mall. Several startups are developing indoor localisation technologies to be able to target users location very precisely, e.g. when entering a specific shop or even when facing a specific shelve, say sodas or cereals, to be able to send or display the right promotion at the right time.

In all cases, what the industry should put first is the trust of the consumers, because in the long run everything relies on the fact that the consumers trust the companies they're trading with or they're involved with, about the fair use of the data they leave behind, again explicitly or implicitly. Therefore, data protection is also a major issue: beyond opt-in and sensible use of the data, we must protect personal data against accidental leakage or fraudulent access by unauthorised internal staff or hackers.

Big Data

Big Data is the new buzz word. It is basically the fact that it is now possible to store huge amounts of data, and with the help of new types of databases and query tools, it is possible to access new levels of customer knowledge, behaviour patterns, etc. It is now possible to accumulate data that were previously not accessible and/or not stored. Let's take every single purchase by every single loyalty card holder in the retail business, or the minute by minute location of a car equipped with a connected GPS. It questions one major statement in the European privacy regulation: that "there is a specific purpose to each data base."

Big Data relies on the assumption that data should be stored for the sake of finding useful information in the future by analysing them with these new powerful tools.

To protect privacy while still be able to tap into the potential of Big Data, the link with the individual who is associated to the data needs to be cut. To do this, one solution is to apply a two stage process to the data. First stage is to anonymise the data, by changing the identifier of each user into an alias, so there is no way to trace back the individual linked to the data. In the second stage data are aggregated so no individual data are stored anymore. Today already some form of BD is used, to model road traffic and therefore find out where there are traffic jams, for real time alert purposes of for analysis and planning of public transports and roads. The root information is the individual movements of cars that can be deducted from the movements of all SIM cards in a given territory, or from all connected GPS.

Use of BD will go far beyond in the future and will trigger new privacy questions. We see that an increasing number of mobile applications and devices offer to monitor simple biological variables (pulse, weight, body temperature, blood pressure) and lifestyle variables (distance walked every day, physical activity, food/calories eaten…). When speaking of private data and privacy, health related data are paramount; as a consumer I consider it strictly private. In fact, all these data are also likely to be accumulated over time and will trigger new possibilities in the future. A user of such service might receive an alert because his daily values are exiting the "normal" values defined by analysing the mass of data available from all users. In that world, I am warned that I might be "sick" before even feeling sick and experiencing symptoms. Several startups have already started to produce such devices, some of them for casual use and some with real/critical health applications in mind. Some have already said that they will never sell individual data…

Identity

Identity is closely linked to privacy. We know that there is a big need for secured identity in the digital world. I need to identify myself to look at my bank account and to transfer money from my account to another account. I want that identifier to be secure enough so that it is not possible for fraudsters to access my personal data or – worse – my savings. And even if my identifier is compromised (lost, stolen) I want my bank to be able to detect (authenticate) that the person using my identifier is not me. This often requires some overhead for the user, such as changing passwords regularly, choosing secure passwords or even using a temporary password received on the mobile phone or generated by a dedicated device, rather than using a simple and unique permanent password. So we must educate our customers to protect their privacy and accept that protection may add some complexity to their daily online life.

Identity also provides a way to increase the trust in digital services while keeping privacy.

A lot of online platforms operate in the so-called C2C or consumer to consumer space. They act as mediators between two individuals: match-making sites, billboards for car selling, holiday home renting, etc. Let's use the example of a billboard website: billboards are generally anonymous until the transaction is ready to be executed, e.g. sell a car. But there are risks in trading with someone acting with a hidden identity, and fraudsters and crooks are plaguing the digital space. In a C2C platform, trustable identity is needed to assert a certain level of knowledge of the parties to a potential transaction. It is not disclosed at first hand, but both the buyer and the seller know that the platform has enough information about the other party to safely engage in the transaction.

We have many digital identities, almost one per service we use, and often weak identities that can easily be compromised. For the sake of simplicity for end users (one universal identity) and to develop a trustable identity framework that effectively protects privacy, the French government (Caisse des Dépôts et Consignations, CDC) and a handful of large corporations (the French post office La Poste, the banking Groupe CIC, the SoLocal Group, and the telecommunications company SFR) are cooperating to define and develop such an interoperable digital identity. This initiative is called IDENUM.

Conclusion

We have tried to illustrate how personal data, privacy and identity are at the core of the digital lifestyle. At the heart of most business models of free online services is customer knowledge, and careful use of customer data improves relevance and performance. Mobile and tablets are increasing usage levels and develop access to services everywhere and all the time. The ability to locate creates additional targeting possibilities. Big Data is a new frontier where previously untapped data sets are used to increase customer knowledge and create value for businesses as well as the public sphere. All this has to be done while letting our customers control their privacy and protect their data against unwanted use. Trusted digital identity is needed to adequately protect the users against fraudulent access.

Pierre-Emmanuel Struyven *is VP Innovation and New Markets at SFR. He joined SFR in 2009. Prior to SFR, he was CEO of Streamezzo, a startup active in application software development for mobile devices. Pierre-Emmanuel spent five years with the world's largest music company, Universal Music, heading operations, product marketing and business development for the group's Mobile subsidiary and Digital division. There he was involved in mobile and digital music business development, with a focus on new mobile distribution channels, customer experience, product development and innovation. Previously, he was director of Product Marketing in the telco industry, and held various positions in IT. He graduated from Université Libre de Bruxelles (Ecole Polytechnique).*

The Future of Privacy in the Internet Age, a European Perspective

Thibaut Kleiner[1]

"Much Big Data does not concern individuals. For data that does concern people, we need firm and modern data protection rules that safeguard this fundamental right. And we need digital tools to help people take control of their data, so that they know they can be confident to trust this technology." (Neelie Kroes[2])

According to many observers involved in Brussels' public affairs, the draft European Data Protection regulation represents one of the most heavily lobbied files of the Barroso II Commission and also the ground for confrontation between EU and US approaches to privacy.[3] At stake is the need to modernise data protection rules in the EU and to make them fit for the digital age. Technological developments are opening new grounds for collecting vast amounts of personal data and individuals are increasingly keen to share online about their private lives.

The prospects to create new services, new applications and new growth in Europe from Big Data are real. Yet demands for increased privacy in the Internet age remain very vivid and received additional attention after the revelations of Mr Snowden about the scale of the US authorities access to digital personal data, in particular through US Internet companies. This article looks at some of these considerations from a European perspective and highlights possible solutions currently under discussion.

[1] Disclaimer: The author is an official working at the European Commission. The opinions expressed in this article are those of the author and do not necessarily reflect the views of the European Commission.

[2] Speech "Big Data for Europe" – Speech/13/893; 07.11.2013, Vilnius.

[3] See for instance, "Europe moves to shield citizens' data", J. Kanter, *The New York Times*, 17 October 2013, www.nytimes.com.

1. New trends in the use of data

In the Internet age, privacy is likely to become a paramount issue in terms of control by individuals and in terms of trade-off between releasing personal data and obtaining services and products that use personal data. Every day, trillions of data are produced on the Internet, from data captured through sensors, to content produced online by individuals and companies – including through social media –, to online statistics, to data collected through credit cards and other marketing channels, to search records and answers, to surveys. Not all this data is personal data, but a fair proportion is. And this data is increasingly collected in a systematic manner and analysed through data-mining technologies. Three trends in particular can be highlighted which could combine to deliver great potential future growth: Big Data, cloud computing and the Internet of Things.

Big Data is a new phenomenon linked with the ability to collect and analyse very large amounts of data, to support decision making and to create value for new or more tailored products and services. Examples of emerging applications show the high potential of Big Data for business. For instance, healthcare companies can benefit from analyses of drugs that are on the market to analyse the effects of these drugs and find possible new benefits. This means improving treatment and reducing costs. New drugs and treatments can also be invented from analysing the vast data to establish genetic influence on certain diseases and possible cures. For instance, the US startup Bina is trying to develop new tailored cures for cancer or infant mortality, applying Big Data analytics to genomics, making it possible to sequence the human genome in a matter of hours rather than days or weeks and to study its link with specific diseases. McKinsey considers that Big Data will have a profound impact on healthcare costs and quality in the coming years.[4]

Big Data can be used by companies to better understand consumer preferences and to propose tailored products and services as a result. Social media offer a mine of data, from discussions about specific topics to queries and opinions about products and services. All these elements can be processed by data-mining companies, which are then able to provide insights about the perceptions of customers. This can be very useful to predict customer behaviour and reaction to the launch of a new product for instance, or to develop products and services that correspond better to their needs. For instance, the song identification company Shazam helps record labels to find out where music sub-cultures are arising by monitoring the use of its services, including the location data, and where they can as a result hope to find upcoming

[4] Groves et al., *The Big Data Revolution in Healthcare*, McKinsey & Company, 2013.

talented artists.[5] Big Data has also many applications in terms of optimising processes. SAS reports that it helped a major consumer electronics group to drastically reduce fraud by combining information efficiently across the company's IT system.[6]

The effectiveness of Big Data is not only coming from the quantity of information, but also from the quality of the data and how well it is curated. Very often, the Big Data approach requires that data sets are allowed to enrich each other from different sources, often private ones. This may require being able to recognise the data subjects to merge the data sets. Companies may need to access data from third parties, e.g. business partners or customers, and integrate them with their own data, to pool together and obtain data with greater analytical properties. How this can be organised in full respect of data protection rules is not a trivial question.

Big Data can be combined with cloud computing and Internet of Things to deliver its full potential. With cloud computing, data can be gathered through the Internet and stored into servers with enormous capacities, where they can be analysed effectively, possibly thanks to supercomputers. This makes it possible to collect vast amount of data and to avoid being limited by the capacity of local computers and servers. With the Internet of Things, objects can be equipped of sensors and transmit a series of data that are then collected and analysed. This makes it possible to improve the reliability of machines, for instance, by controlling the durability of the parts and being able to change them before an incident occurs, thus reducing maintenance costs. For instance, US manufacturer John Deere uses sensors added to their latest equipment to help farmers manage their fleet and to decrease downtime of their tractors as well as save on fuel. The information is combined with historical and real-time data regarding weather prediction, soil conditions, crop features and many other data sets.[7] Connecting objects makes it also possible to track the performance and usage of products and to collect data about how they react and how they are actually used by customers. Thanks to data analytics, it is then possible to improve the user-friendliness and customer experience and to invent new applications too.

2. Challenges for privacy

These new trends run into important questions as regards privacy and ethics. Technology becomes so powerful that data elements that would not

[5] Datascience, "Ten Practical Big Data Benefits", *Data Science Stories*, 2012, www.datascienceseries.com.

[6] Spakes, Gary. "Four ways Big Data can benefit your business", *SAScom Magazine*, third quarter 2103.

[7] See MyJohnDeere.com.

reveal much if they remained separate suddenly can be made very telling if they are combined and analysed on the basis of broader statistical evidence.

The company Target for instance became known after an article in *The New York Time*[8] revealed how it could identify a pregnant woman, in that case a teenage girl, without their parents knowing about the pregnancy. The statistician at Target explained that the company had developed through Big Data some statistical indicators about purchasing patterns that would allow to identify a pregnant woman and to propose her targeted products before she would give birth. This anecdote shows how the sensitivity about Big Data is making it possible to find out about your inner secrets without you necessarily wanting to share this information.

In broader terms, technology raises challenges about the control over data and its applications. A key principle of data protection regulation in the EU is the notion of consent, which is one of the legal grounds that allow processing of personal data. EU legislation specifies that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. However, it is not clear whether this is easily delivered in the case of data generated automatically and processed through data-mining technologies, as it is not obvious what the ground for processing may be *ex ante*. Similarly, in case of innovative mobile applications based on the Internet of Things, the nature of the data and whether it is personal or not may be contested.

To make things even more complicated, one should also underline that privacy may be evolving in society at large. With the development of social media, individuals are increasingly becoming public figures on the Internet. The Eurobarometer survey showed that 74% of Europeans think that disclosing data is increasingly part of modern life, but at the same time 72% are worried they give away too much personal data.[9] Interestingly, Febelfin, the Belgian Federation of Financial Institutions, hired an actor to pose as a mentalist, while he was actually only taking advantage of information these people had posted on the Internet, revealing to them how their privacy was possibly infringed through their own actions of sharing it online.[10] Any solution to the novel issues for privacy in the digital age requires for that reason to include users in the equation.

[8] Charles Duhigg, "How companies learn your secrets", *The New York Times*, 6 February 2012, www.nytimes.com.

[9] Special Eurobarometer 359, "Attitudes on Data Protection and Electronic Identity in the European Union", June 2011.

[10] http://www.febelfin.be/fr/partager-des-informations-sur-Internet-cest-sexposer-aux-abus.

The example of the cookie regulation is in that sense also revealing. In the Netherlands, the legislator transposed the e-privacy directive very thoroughly and introduced obligations for explicit consent. As a result, websites have introduced in the Netherlands specific requirements for users to give consent explicitly by clicking on banners that appear each time there is a new use of the data. The problem of this implementation, however, is that it became not very user-friendly, given the number of times that users have to click on something to simply continue to use the service. Observers even consider that the practice was counter-productive in terms of data protection, because users, in order to be able to enjoy a smoother experience, ended up giving excessive consent to the use of their personal data. A similar concern exists in relation to the very long terms and conditions that Internet platforms ask their users to consent with, whereas they do not provide any alternative (meaning that not consenting to the terms and conditions equates with not accessing the service!).

Finally, there is a geographical dimension in these issues, as data easily flows across borders in the digital economy. This raises the question about what legal framework applies, if the data is processed and stored in a different country, for instance. Given the recent revelations about the activities of the National Security Agency of the United States and its alleged access to massive amounts of personal data of European citizens without due regard to dual process and protection as per European legislation, this issue has become very sensitive in the past months, and questions the need for additional safeguards for data transfers from the EU.

3. Is a radical change in the legal framework necessary?

Considering these many technological challenges, the European Commission started in 2012 a review of the EU legal framework on the protection of personal data. The new proposals aim at strengthening individual rights and tackling the challenges of globalisation and new technologies.

The right to personal data protection is recognised by Article 8 of the EU's Charter of Fundamental Rights. The right to the protection of personal data is also explicitly stated in Article 16 of the Treaty on the Functioning of the European Union. This gave the EU new responsibilities to protect personal data in all areas of EU law, including police and judicial cooperation. In Europe, legislation on data protection has been in place since 1995. The Data Protection Directive guarantees an effective protection of the fundamental right to data protection. The current rules, however, were introduced at a time when many of today's online services and the challenges they bring for data protection did not yet exist. In fact, the current rules very much derive from the OECD principles (and can be traced back to the 1953 European Convention on Human Rights):

– Notice: Data subjects should be given notice when their data is being collected.

– Purpose: Data should only be used for the purpose stated and not for any other purposes.

– Consent: Data should not be disclosed without the data subject's consent.

– Security: Collected data should be kept secure from any potential abuses.

– Disclosure: Data subjects should be informed as to who is collecting their data.

– Access: Data subjects should be allowed to access their data and make corrections to any inaccurate data.

– Accountability: Data subjects should have a method available to them to hold data collectors accountable for following the above principles.

The data protection reform has set a series of objectives. A reinforced "right to be forgotten" was proposed to help people better manage data protection risks online: People will be able to delete their data if there are no legitimate reasons for retaining it. Wherever consent is required for data to be processed, it is proposed that it is given explicitly, rather than assumed as is usually the case now. In addition, people will have easier access to their own data and be able to transfer personal data from one service provider to another more easily. There is also increased responsibility and accountability for those processing personal data: For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible, within 24 hours). People should be able to refer cases when they are victims of a data breach or when rules on data protection are violated to the data protection authority in their country, even when their data is processed by an organisation based outside the EU. In addition, it is proposed that EU rules will apply even if personal data is processed abroad by companies that are active in the EU market. This will give people in the EU confidence that their data is still protected wherever it may be handled in the world.

However, the proposal has led to a heated debate. In particular, a number of private sector companies warned that while they shared the objectives of the proposal, the solutions developed to meet them raise a series of difficulties linked with their suitability for the online business. The worries of many Internet companies or of companies involved in cloud computing and Big Data are that this new framework will make a number of existing business models difficult to operate and that it will create new rigidities for business, with risks of very high fines in case of non-compliance having the potential to freeze experimentation and innovation. For instance, the obligation to ask for consent before analysing data as well as the prohibition of profiling have been raised as major hurdles.

The American Chamber of Commerce to the EU – a good proxy for the position of the US digital businesses – underlined that making explicit consent the norm will inhibit legitimate practices without providing a clear benefit to data subjects. It believes that profiling techniques *per se* do not need special regulatory treatment given the many safeguards in the draft Regulation. At minimum, the Regulation should make clear that the restrictions on profiling do not extend to beneficial activities such as fraud prevention, service improvement, and marketing/content customization.[11] Another issue is the "right to be forgotten." Among others, Facebook criticised the proposal saying that it raises major concerns with regard to the right of others to remember and of freedom of expression on the Internet. They also pointed at a risk that it could result in measures which are technically impossible to apply in practice and therefore make for "bad law."[12]

The Council to that day has not managed to develop a negotiation mandate. One of the most contentious issues is whether a one-stop-shop would be maintained or whether national governments would want to maintain national regulators for the activities on their territories. Potentially, this could largely burden compliance and take away the objective of creating a single market for data. In Parliament, more than 4,000 amendments were proposed to the text through various committees. Discussions were very heated, but on 21st October, the lead committee (LIBE) managed to adopt its report (prepared by MEP Albrecht). A series of elements are introduced and notably the notion of pseudonymous data, which is proposed to be subject to a lighter framework. The definition of consent is slightly relaxed, as statements and actions are included as a proof of consent. New provisions are introduced for international data transfer: notification for data transfer or disclosures and propose that all adequacy decisions (such as the Safe Harbour decision with the US) expire five years after adoption of the regulation. It proposes to introduce a European Data Protection Seal, and increases the amount of sanctions in case of non-compliance to €100 million or five percent of worldwide turnover.

The processing of health data for research, statistic or scientific studies is still authorised but data controllers would have the obligation to obtain

[11] AmCham EU position on the General Data Protection Regulation; 11 July 2012; American Chamber of Commerce to the European Union; Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium https://dataskydd.net/wp-content/uploads/2013/01/AmCham-EU_Position-Paper-on-Data-Protection-20120711.pdf.

[12] http://thenextweb.com/facebook/2012/11/20/facebook-proposed-eu-right-to-be-forgotten-raises-major-concerns-over-freedom-of-expression-online.

consent from the data subject. Last but not least the Albrecht report proposes to get rid of the notion of "right to be forgotten" and replaces it with the right to erasure. In addition, the Commission's proposal already restricted it in some cases, for instance when the data are needed to exercise freedom of expression, for public interest in public health, for historical, statistical and scientific purposes, or when required by law.

Also, it is worth noting that the Commission published a Communication as regards international transfer of data as a consequence of the new challenges highlighted by the Snowden revelations[13]. The studies found a series of shortcomings, in particular about companies who had wrongfully declared they were listed but were not, or those who did not correctly publicise the principles. Also some companies did not implement the principles in their actual corporate policies.

Finally, reliance on self-certification led to inadequate level of enforcement. Furthermore, the large scale access by intelligence agencies to data transferred to the US by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data in transferred to the US. On that basis, the Commission called for improvements in the Safe Harbour decision, notably in relation to enforcement by the US authorities and obligations of private companies.

4. Future possible avenues

It is clear that technological developments are challenging the established legal frameworks and raising novel questions. At stake are difficult issues linked to the balance between privacy and growth. The European approach, however, is one where both are preserved.[14] Possible avenues have already been outlined, which require some further investigation and testing.

First of all, as regards the issue of consent and notably the limitation of the possibility to process data without obtaining informed consent, there are possibilities to transform the data, either through anonymising or pseudonymising it. Anonymous data should normally preserve privacy, but it may not allow significant meshing and combination of datasets, which is precisely the novelty in the Big Data approach. The notion of pseudonymous data may offer better possibilities. The EC proposal of Data Protection Regulation does

[13] Communication from the Commission to the European Parliament and the Council, Rebuilding Trust in EU-US Data Flows, COM(2013) 846.

[14] See e.g. Viviane Reding, "The importance of strong data protection rules for growth and competitiveness", European Commission - SPEECH/12/171 01/03/2012. Neelie Kroes, "The Big Data revolution", European Commission - SPEECH/13/261 26/03/2013.

not contain provisions on pseudonymous data. However, the new article 4(2a) proposed by the Parliament sets out the definition of "pseudonymous data," which means: "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution."[15] Pseudonymous data would enable some further processing without needing new consent, which would benefit to Big Data analytics. Transforming data in such a way should be possible if the data is of sufficient quality and recognisable. In case this data would be de-anonymised, due for instance to the combination of several data, the lawfulness of proceedings would, however, still depend on the presence of consent.

Another opportunity could result from clearly sequencing the collecting of consent from further processing, as suggested by the Article 29 Working Party (WP29) opinion 03/2013 on purpose limitation. Data analysis is not problematic as long as the data controller does not find personal data. So data about machines, for instance, should be processed without difficulty. Once the collection of personal data occurs, data protection rules have to apply and either consent or the allowed exceptions may be used for further processing. The WP29 emphasises that the specific provision in Article 6(1)(b) of the Directive on "further processing for historical, statistical or scientific purposes" should be seen as a specification of the general rule, while not excluding that other cases could also be considered as "not incompatible." This leads to a more prominent role for different kinds of safeguards, including technical and organisational measures for functional separation, such as full or partial anonymization, pseudonymization, aggregation of data, and privacy-enhancing technologies.

Thirdly, privacy impact assessments may offer opportunities to identify risks and to provide remedies to innovative and novel issues as regards privacy in a new context, such as Big Data or cloud. These impact assessments could be conducted in a way that is transparent and coordinated with the authorities, to avoid excessive burden on individual companies. They would offer a space for discussion about emerging risks, and for tailored solutions that could be flexibly amended over time.

Along the same line, there is certainly scope to use technology in a better way, so that it delivers privacy by design. Too often, privacy is a secondary consideration, and it operates as a remedy to a technological problem. By integrating privacy from the outset in the technical specifications, it is possible to

[15] Compromise Article 4, available at http://www.edri.org/files/eudatap/04COMPArticle04.pdf.

limit the legal barriers to data processing. For instance, the initiative around Do-Not-Track[16] offers possibilities for users to stay in control about what data they share through their browsers. Developments around automatic deletion of personal data through apps, or default restriction to the transmission of personal data can be developed.

Furthermore, there may be scope to support the development of compliance models akin to Binding Corporate Rules to increase accountability at the level of individual data controller, thanks to standardisation and certification processes. Binding Corporate Rules (BCR) are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. It may, however, be possible to normalise the processes that underpin BCR and to develop standards that can generally be applied at industry level. This would develop alternative mechanisms for businesses to comply with privacy, through industry standards that could be validated by data protection authorities, and maintained through specific audit procedures. Such an alternative model could offer additional flexibility and scope for innovation.

Finally, whatever solution is envisaged, it is essential that users are kept in mind. User-friendliness is essential to deliver good results, and it is important that sound principles are translated into operational and feasible steps that can be mastered by users. The example of the cookie regulation and its implementation in the Netherlands is a good example in that respect: while the spirit of the law was very commendable, the way it was implemented led to unpractical and cumbersome processes, which have created irritation among users and excessive consent. Using behavioural economics and testing of technological solutions would therefore seem a useful development in the field of privacy and data protection. Here again, dialogue between industry and data protection regulators should be paramount.

Thibaut Kleiner *is a member of the Cabinet of Vice President Neelie Kroes, European Commisison. Thibaut is a senior advisor in charge of Internet policies (privacy, Internet governance, media and data, etc.). He has been working for the European Commission since 2001, occupying a number of positions, notably in the field of competition policy, where he was head of a unit in charge of coordination, and member of the cabinet of Neelie Kroes during her previous mandate, where he notably supervised state aid (including during the banking crisis). An economist by training, he holds a Master from HEC Paris and a Ph.D. from the London School of Economics.*

[16] See e.g. http://www.w3.org/2011/tracking-protection.

Value Creation and Privacy

How Does Personal Data Valorisation Happen?[1]

Nicolas de Cordes

Personal data valorisation is happening through a complex and vibrant value chain. It is first collected through various means: mobile phones' OS or their apps, computers, communication networks, social networks, electronic notepads, readers, smart appliances, smart grids, sensors, etc.

It is stored, aggregated, processed and then exchanged by Web retailers, Internet behavior tracking companies, search engines, electronic medical providers, identity providers, network operators, Internet service providers, financial institutions, utility companies, public administrations, etc.

Personal data have typically three different origins: Volunteered when users declare their interests and preferences; observed through monitoring of usages: browsers history, consumption via credit cards or online shopping, search and localisation requests on maps, etc.; finally it can also be inferred or deducted, when algorithms and crossing of different data sources create new attributes and profiles of users for different purposes.

The end users of personal data usually are the companies serving the users in the first place, but also third parties looking to commercialise or serve better their customers by enriching their knowledge (companies, government agencies or public organisations), and increasingly the users themselves, who can reuse these personal data to improve their services.

All told, the value created through digital identity and personal data can be massive. A BCG study estimated a 22% annual growth rate of business directly related to personal data, which could deliver a €330 billion annual economic benefit for organisations in Europe by 2020. Individuals would benefit to an even greater degree, as consumer value will be more than twice

[1] Transcription of the speech given during the Privacy seminar of Institut Mines-Télécom.

as large: €670 billion by 2010. The combined total digital identity value could amount roughly to EU-27 GDP (1,000Bn€). But, as many analysts, BCG estimates that two-thirds of this potential value generation is at risk if stakeholders fail to establish a trusted flow of personal data.

How companies monetise data

The analysis that makes valorisation and monetisation out of data possible has existed for a long time. What is different now with Big Data is that *data has become a product.* There are all sorts of products: One can use Big Data to find a parking space, to improve transport, to certify someone's identity or their relationship with someone else, to identify hot spots of criminality and help the police make the place safer, to facilitate recovery in case of a disaster; if you have a big problem in a country like in Haiti, what can you do to help public services restore faster and help people? There is also the consumer side: In China you can track in real time your parcel being delivered at home; you can call the guy on his bicycle and tell him "I'll be five minutes late, please wait for me." An example of that at Orange is one of our upcoming products, Flux Vision, that proposes the analysis of tourist flows, which we already applied in the South of France.

Of course, potentially, as everything goes faster in the digital world and is increasingly based on automated algorithms, things might lead to sensitive situations. One famous example is how Target, a US retailer, identified a pregnant woman because she suddenly changed her consuming patterns. She was suddenly buying fresh food and yoghurts instead of eating chips and potatoes, and drinking water instead of Coca-Cola. The father discovered her daughter was pregnant because she received advertising in their loyalty programme that was "bizarre" for her.

So, there are some new questions about "where is this all going?" abundantly relayed in the press that give you the gist of the complexity of the subject: "PayPal is going to share the data of its users with Facebook, Criteo, Mediaplex and others. In opt-out"; "How iPhone apps suck up information about you without you knowing"; "Germany: widespread theft of data at Vodaphone"; "Facebook: one more controversy about provacy"; or the "Prism" scandal.

But things haven't always been so.

A dynamic view of the situation

In the past, exchanges between people through conversation and letters, were usually, and "by default," informed and consenting. Each party knew what information they gave and received. In the 1980s, personal computers appeared. There was still informed and consenting exchanges of information, and you voluntatily declared some data. Things became a bit more complex in the 1990s when computers started to be more connected and exchanges more automated. Servers were talking to other servers, all of them trying to enrich the system which made inferences about people. Things became even more complex in the 2000s with the rise of the Web 2.0 and social networks when people got even less aware of the fact that they could be observed and their social network was giving information about them to third parties. Then we entered the 2010s and things became really complicated, people started to get lost in complexity of services interconnections, overwhelmed by data, to the point where now nobody knows what is going to happen and where all this is going to lead us.

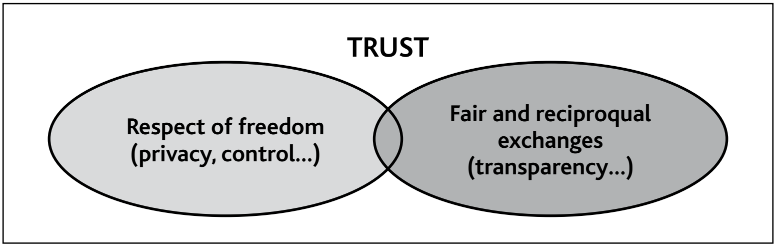
So, what is really different? There is a traditional definition of Big Data called the "three V": "Volume, Velocity, Variety" that gives a technical definition of it. But we can try to analyse the way the less digitally comfortable consumer or the layman in the street might perceive the situation: "Volumes: Well, things are constantly collected in volumes that I cannot even fathom, there are bizarre thing I don't understand, the zeta and beta bases, I have no idea what they are. The speed at which things happen don't allow me to intervene in the process, I'm not capable of stopping these things from happening. A variety of crossing sources make inferences about me that I'm not aware of, even if I might disagree with them. They suppose things about me and I don't know what they are... nor do I know how I could be informed about it and correct them, or erase them if I want."

This is creating the sort of situations we see in newspaper or in interviews with our customers, where people start having serious worries about abusive and discriminating use of their data, with the immediate risk of losing their trust. The word "trust" is often mentioned and I think it is a very important thing. As a business, trust is the basis of the relationships between a company and its clients and partners.

Trust is fundamental; it is the basis of society. If there is no trust, countries end up with civil wars; there would be no real economy, no banking system for instance because people would be only pre-paying with small cash. These are obvious consequences of not having trust. Now, as the digital world increases, some governments say we will be digital by default: Trust in a digital economy is obviously something very important.

Trust in a digital society

Trust is based on the mutual respect of the right to Freedom of action and on expecting fair and reciproqual exchanges of "values."


TRUST
Respect of freedom (privacy, control...)
Fair and reciproqual exchanges (transparency...)

Trust is the basis of society: It brings social stability instead of unsecurity and erratic behaviour; it brings forth economic development in place of small-cash-based economy. Also, trust enables law, bills of rights and democracy that must prevail over the rules of the strongest.

But trust is slow to build. One major question concerning the use of Big Data then, is: Is trust at risk in digital societies? At present, 60% to 80% of people express a lack of trust in some form when talking about their personal data. Loss or lack of trust in the digital world is not a good sign for our society which is going "digital by default."

In a non-expert – legal, philosophical, or linguist – view of the question, trust is both a feeling and an attitude based on two major principles: One is the respect of the freedom of the individual or the party we are talking with, the other one is to have a fair exchange, something that to your eyes seems fair and non discriminatory. The second principle, the notion of privacy, is something very important that takes several different forms. One element of privacy is linked to the emergence of automatization and algorithms that are creating a world which is a little at risk of becoming algorithm-centric instead of user-centric. So, privacy, because of its two critical applications, protecting citizens against abusive government and protecting consumers against unethical business, is central...

Privacy in the digital world

In the Internet world, Freedom of action requires both parties to respect Privacy – control of disclosure of ones' identity(s) and data for a contextual use – and to offer some transparency to guarantee fairness and non-discriminatory treatment. Secrecy and Intimacy are close relatives of Privacy, with their own needs and cultural values (Individual vs Group value, historical background to protect individuals, etc.).

Like Freedom, Privacy is difficult to define; data about one's identity(s) is considered personal dependant on context…

But Privacy is important:

- By enabling the opacity of the individuals, Privacy protects against the infrigement of the state, companies or fellow citizens.
- Misuse of personal data can be damaging in many ways: segregation of insurance, bias in recruiting, reduced medical help, social pressure, loss or usurpation of identity…
- Enabling better level of personal data control over the respect of intentions would also help resist the emergence of algorythm-centric approaches that are already transforming the society, in favors of customer-centric approaches.
- Privacy becomes more precious, as objectives of economic performance tend to increase profiling discrimination for customers or citizen services.

Value in the digital world

Exploiting the value of personal data is already happening, in an extremely complex value chain with hundreds of thousands of actors from very large to very small. It is a very complex chain indeed you will need to address if you want to modify something. The value we are talking about is reaching 1,000 billion euros in Europe according to the study mentioned before. Whatever that number means, it is gigantic and we can be sure there is a really big interest for looking into and controlling some parts of the value of this data.

Personal Data can be exchanged for a clear benefit like free access to a service, or receiving a coupon, or the finer personalization of a product. But when we look at whether people are ready to specifically sell information themselves for cash, and at how much they will be ready to sell it for, we can see that the proportion of people ready to share information goes up with the price going up. But not that much… At one point it reaches a plateau. Obviously something else is going on.

A BCG digital identity survey shows that customers can put a price on their data, but not the same price on all data: the price is fairly low for age group and gender, opinion on products, e-mail address and main interests (€5 per month minimum for 50% users), not so low with more sensitive data such as past purchases, purchases plans, media usage and location (€22 minimum for 50% users), and would have to be quite high for social network posts, medical records, financial data or credit card data (for all users, €50 wouldn't be enough). More than half the people would not agree to voluntarily give very sensitive personal data even with financial compensation.

What is going on could lead us into the problem of privacy from a different angle. The concept came from the behaviour sciences: During exchanges it seems that people have two accounting or value systems operating in their minds. First there is the social accounting or value system: "I give you something, you give me something and we find it fair." Second is the economic accounting or value system: "If I give you one euro, I expect to receive one euro or one euro plus something." This sort of balancing act really takes place in our heads, and behavioural sciences teach us that we cannot mix those two value systems. If you give a nice book, a gift to someone and say: "Here is something I found for you, I like what you read, I thought this book would be really interesting, and by the way, there was a discount and I got it for 10 euros only…" Take another example: You are at a family dinner, your stepmother has made a fantastic lunch, everybody is happy, everything is really nice; now you take your wallet and say: "Dear stepmother, it is so fantastic I will pay you 150 euros for this dinner…" That doesn't really fly. If you ask your neighbour to help you carry and transport some very heavy thing, he will be happy to do it if there is just the one thing and if he is on his own with you. But if at the same time you have your movers around, whom you pay, and you ask him for help (without him being paid obviously)… It doesn't work. In these three examples, we are mixing social exchanges and monetary exchanges.

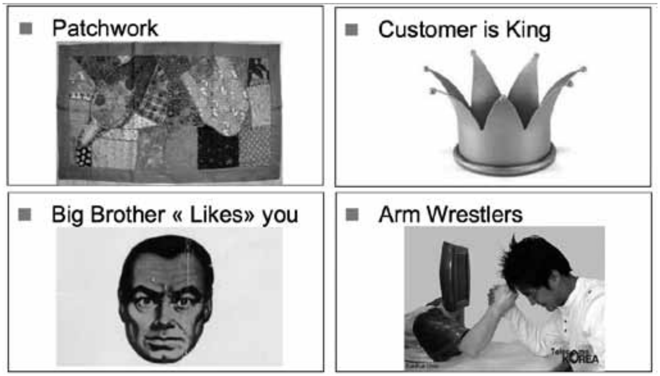
What is true between people is also true between companies. Imagine a bank that would say: "We are a family business, we love our customers, everybody is part of a big family." Then, if you have a problem of payment and you go and see your banker, what you would expect to hear is: "Oh, I'm terribly sorry for what's happening to you. What can I do? Let's stop the reimbursement process immediately. Come back whenever you are ready." You would expect this kind of friendly family attitude. But the banker would more likely say: "It is annoying you are only half way through your loan, maybe I can lend you a bridge loan, and maybe I can take some mortgage on your car." Mixing the systems obviously cannot happen.

The evolution of the concept of monetising personal information is confronted to that problem. A first exchange of information takes place in one purpose, then this information is repackaged, and when it is repurposed for another usage which involves money, this clearly touches the two very sensitive accounting system we have in our heads. This is one of the reasons why we are stuck with the personal data problem. Reconciliating the monetary and social aspects of the value system is really something important and it may appear to be less about exchanging monetary value or giving people a share of the deal, and more about giving the opportunity to users to have some level of control. What I mean is that we absolutely need to respect the context and the personal intentions, and this is a particularly difficult problem.

This analysis can be seen as a sort of basic level, a background context for looking a little further into the future.

Privacy scenarios

When we talk about scenarios, we typically look at trends, then we see what is the common agreement about things and what are the variables, what could go in one direction or the other. This usually requires a lot of thinking and brainstorming. Here is a scenario landscape:



- Patchwork
- Customer is King
- Big Brother « Likes» you
- Arm Wrestlers

(UL) Patchwork:
– Creative silos, a world of Mini Data and alliances
– Users' assemblee services that work together linking them through IDs
(UR) Customer is King
– User-centric permission Web architecture
– Personal data lockers used as foundations for ergonomic personal services
(BR) Arm wrestlers
– Strong policies and law enforcement create users' counter power
– Users manage IDs and privacy settings
(BL) Big Brother likes you
– Oligopoly, GAFA + IDs
– Large commerce platforms drive the digital world with a 360° view of their customers

On the horizontal axe is the possible evolution of control by the user over its personal data, with respect of context and every other safeguards, and forms of control which might not exist yet, or start to exist on a small scale. On the other axe is something we haven't talk much about, which is commercial power and competition structure. Do we have a market concentrated on a few very powerful actors or do we have a more fragmented situation with many small players?

So we have a bit of a demand-and-offer landscape for privacy scenarios. We imagined scenarios in that context, privacy laws on one side, competitive laws on the other side, and they are linked. These types of scenarios are very simplistic views, landscapes; they show the extreme options.

On the bottom left, we find the "Big Brother likes you" box. This is a bit of a frightening sort of future. To some extent, there is a natural gravity driven by the power of the platforms and the power of the economics which tend to drag the system down into that box. There is a natural monopoly in the way the network operates that naturally intends to go in that direction. This is why we need to go away from that box by educating people, by making regulations evolve and by finding ways to go elsewhere. Unless we are happy with a "Big Brother" scenario... Going elsewhere is a choice of society. I'm not going to promote Orange opinion on cultural value and social decision. Which direction we take is a political decision, to be taken by us as citizens. However, Orange has an opinion about what would be good for its own business. And we don't like much this extreme bottom left corner where all the information ends up in a situation which is not good for the global dynamic of the ecosystem. We obviously prefer an environment with a balanced view of the different actors where the user has more things to say because that will be a better basis for creativity.

We know there are a lot of regulation levels, things that a regulator can do from bills of rights to political debate about automatic actions, trust-based standards, emergence of third parties, and privacy by design and so on. These are all the levers we could use, these are indeed the tools that are under discussion to move the position into a more favourable scenario.

To sum up...

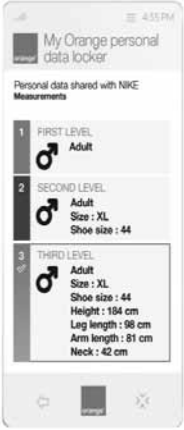
We need to increase our chances to evolve in the right direction for a better balance of power between users and companies and institutions. A regulatory and policies tool-box could use many approaches to that effect:

– Propose a Bill of Digital rights, fit for the XXIst century.
– Organise the political debate about "discriminatory" automated profiling.
– Encourage private trust-based standards (charters...).

- Enable the role of third parties (certifyers…).
- Promote "Privacy by design" approaches (consent, context…).
- Develop ergonomic graduated consent, avoid manipulation.
- Discourage mixing of social and economical values.
- Increase user perception of privacy as a society value.
- Encourage portability of personal data, and personal data managers.
- Force disclosure of breaches, and install fair penalties.
- Reduce digital divides (anonymity, filter bubbles…).
- Address technical issues (by-pass and trust architectures), etc.

What Orange does and doesn't do

What does Orange do about this? Orange could have waited for the regulators to push proposals, but obviously we didn't. We have been developing for the last two years a strategy about what we do with customer data. There are three dimensions to our strategy: The first one is about using data to improve our service for the customer and our own operations while fully respecting their privacy. This is the basis and it is written in our contractual terms and conditions. When you sign up with Orange, you can legitimately expect that we will do our best to improve the service we offer you, and that goes through leveraging the data we collect for and from you. The second dimension is giving back the data to the customer. Helping him enjoy a more fruitful, effective, and dynamic life in the digital world because he can access his information and reuse it to some extent. This is a proof of trust and of a balanced relationship we will foster. The third dimension is using data for external services. This is where we have to be much more careful. The priority is clearly the first and second dimensions, this was very clearly stated by the Executive Comity. The third dimension is something we want to progress towards but with extreme caution and together with the regulators, and with a very ethical and careful approach, putting our customers privacy first.



4:55 PM

My Orange personal data locker

Personal data shared with NIKE
Measurements

1 FIRST LEVEL
♂ Adult

2 SECOND LEVEL
♂ Adult
Size : XL
Shoe size : 44

3 THIRD LEVEL
♂ Adult
Size : XL
Shoe size : 44
Height : 184 cm
Leg length : 98 cm
Arm length : 81 cm
Neck : 42 cm

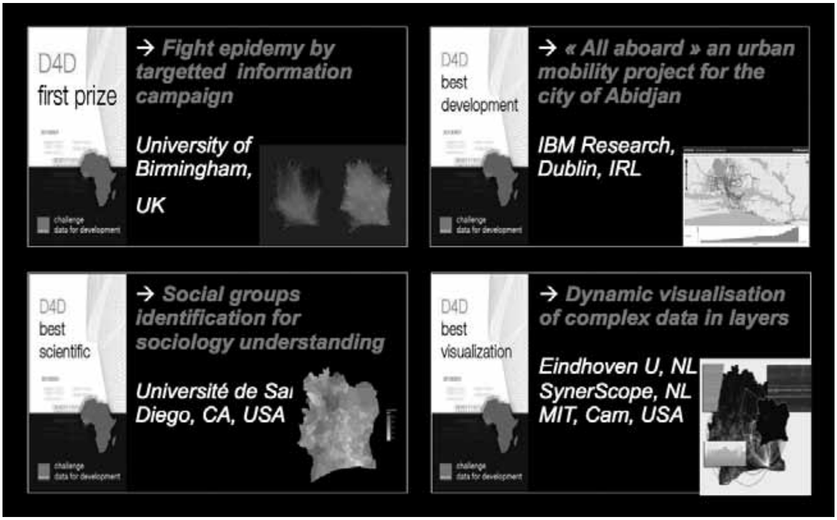
The Orange personal data locker

Another thing Orange is exploring is ergonomics. Ergonomics is a central question in the ability of a customer to do more things about his own data. We designed the Orange personal data locker like a concept car. The concept of the data locker experience is that a customer entering a shop will be able to adjust the level of information that he discloses to the shop to have a personal shopping experience. When he goes out of the shop, he automatically goes back to a safer level. When he enters the shop, he can agree to say for instance: "I will give you my details about sizing because I would like to see only things that fit me," and only sizing details would be displayed.

We set up a data governance board that really help the company manage and define its approach, to "ensure appropriate governance for the protection of privacy and personal data in line with Group strategy, while fostering the focused development of new business opportunities on Personal Data."

Conclusion

Finally some food for thought. So, this is what we do at Orange at present, but we are also exploring the future and we are confronted to big questions, as we all are. First thing – which is also my personal belief: Big Data is a necessity. We might like it or not, but the problems of the world we are confronted to are too big for us to just let them happen. We need to use every resource available to humankind to help solve this big crisis we are potentially facing. And that means using Big Data.



D4D first prize

→ Fight epidemy by targetted information campaign

University of Birmingham, UK

challenge data for development

D4D best development

→ « All aboard » an urban mobility project for the city of Abidjan

IBM Research, Dublin, IRL

challenge data for development

D4D best scientific

→ Social groups identification for sociology understanding

Université de Sai Diego, CA, USA

challenge data for development

D4D best visualization

→ Dynamic visualisation of complex data in layers

Eindhoven U, NL
SynerScope, NL
MIT, Cam, USA

challenge data for development

One of the virtuous uses of Big Data is shown in the results of a contest that we launched in 2013, called "Data for Development" (D4D). We released network information, statistically anonymous information, to the research community. We ask them to try and find how to use this Big Data to help Ivory Coast society to work better and develop. In the upper left corner, we can see that researchers at the University of Birmingham, UK, found a way to reduce the spread of diseases. In the upper right box, we have IBM who did an analysis on how to improve the traffic flows in Abidjan by building an extended bridge. Bottom left is the analysis of social structures and the dynamics of populations and ethnicities in Ivory Coast. The bottom right box shows a price for visualisation.

What I believe is that to some extent, Big Data is a little like discovering a new technology, a sort of DNA of the world. When Crick and Watson discovered DNA, they uncovered a lot of information about living organisms: plants, animals, human beings. If you get hold of this information, you can start to manipulate the living. That information is the source of lot of innovation and value, but also of numerous questions: ethic questions, regulatory questions, setting up chains of control limiting uses and so on. Nowadays, we start to be able to use genetic technologies to improve certain dimensions of our world. Big Data is the same thing in a way. We need to learn how to use all new technologies in a responsible way and make sure we evolve towards a better world.

Finally, I have a question for you all. We are digital migrants. I've been a migrant for some years in the UK, we moved inside the UK for a number of years. When you are a migrant, the first thing you are confronted with is language, you don't master the language. So, there you are, stuck, you almost cannot talk. Then, there are all the small cultural sort of things. We can see how people meet: They shake hands, or they kiss on one cheek like in Belgium, or on two cheeks like in France. We encounter all sorts of little variations, "little" cultural things that don't belong to our native culture: Shall I make a gift? Shall I take off my shoes when I enter a house?

I believe we are migrants in the digital world. So, what can we bring into this new country of adoption, which is a digital world, something good like import-exporting Chinese food or Belgian chocolate from one culture to another culture. What can we bring to the digital world? I believe privacy is definitely, at least in my opinion, something that we should bring from our countries to this new one.

Nicolas de Cordes *has been Vice President Marketing Vision at Orange since 2010. He helps the Orange-France Télécom Group define its strategic marketing direction, recommends new business to enter in, develops future value propositions, explores lateral marketing opportunities with partner companies. Prior to that he was VP Corporate Strategy for the Mobile business of Orange Group in London and VP of Corporate strategy for the Orange-FT Group. He is a civil engineer and graduated from Université Libre de Bruxelles.*

The Place of Privacy-Enabling Technologies in the Evolving Value Chain of Personal Data

Armen Aghasaryan

Privacy versus Disclosure balance

In his seminal work, *Privacy and Freedom*[1] (1968), Alan Westin gives the following characterization to the relation between the privacy protection and disclosure needs: "Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives." Achieving this balance contributes to the protection of democratic processes in the society by preserving a private sphere for individuals as opposed to the public sphere.

Several decades later, in our era of Big Data and cloud computing technologies this balance is perturbed without any commonly accepted means being provided to the consumers of the Internet economy in order to help them find such a personal equilibrium. To illustrate this situation let us consider for instance a conscious privacy-sensitive user of a social network who is provided with a comprehensive panel of privacy protection and personal data disclosure options. Such a user could deliberately select the content before publishing it and will decide which aspects of his personal data to unveil (to the system and to the community) and what to keep private. Now, can one expect that such an ideally configurable environment would allow a privacy conscious user to maintain the Westin's balance? The problem here is that

[1] Alan F. Westin, "Privacy And Freedom", 25 Wash. & Lee L. Rev. 166, 1968.

such a scenario can be imagined only for a silo system, while in today's interconnected world the privacy is threatened by the consolidation of various data sources. This happens for example in the scope of a single large data controller covering multiple service domains (e.g. Google search, Gmail, Google+, and YouTube), where the domain-specific personal profiles are consolidated into a unified personal profile. More generally, the privacy breach can happen by re-identification of anonymised data through crossing data sources from completely different public or private domains.

A well-known example is provided by the de-anonymization attack of a Massachusetts hospital discharge database achieved by joining it with a public voter database.[2] It has been naively believed that simple removal of explicit user identifiers such as name, address, phone number, or social security number would be sufficient to maintain the user's confidentiality within the disclosed personal data records. Very often however, the remaining data can be used to re-identify the subjects of data records by matching them with other data sources. This phenomenon is furthermore emphasised with the emergence of Big Data.

Big Data analytics finds out hidden correlations

Big Data refers to the huge amount of heterogeneous data created through many online sites as well as large offline data repositories. Every piece of digital data that users leave online, their browsing experience, likes, comments, instant messages, emails, status updates, geo tags, or multimedia content, all become part of Big Data. Putting together such a large landscape of personal data allows developing complex data analytics capabilities which makes it easier for businesses to customise their services and fit the users' specific hidden needs. At the same time, Big Data analytics reveal personal information and can violate the users' privacy in many unexpected ways which are out of the user's control. Another well-known example of such a "successful" privacy attack has been demonstrated in the context of the Netflix Prize contest.[3] The world's largest online DVD rental service announced a $1-million Netflix Prize for improving their movie recommendation service. To that end Netflix publicly released the movie ratings of 500,000 subscribers (about 1/8th of its total number of subscribers by 2006) after removing their explicit personal identifiers. While movie ratings might be considered not as sensitive as medical records, the release of such volumes of data raises important privacy

[2] Latanya Sweeney. "Weaving technology and policy together to maintain confidentiality." J. of Law, Medicine and Ethics, 25(2–3): 98–110, 1997.

[3] Narayanan Arvind, and Vitaly Shmatikov. "Robust de-anonymization of large sparse datasets." Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008.

issues. Namely, it has been demonstrated that an adversary who knows only a little bit about an individual subscriber can easily identify the subscriber's record in the dataset. Using the Internet Movie Database (IMDb) as the source of background knowledge, the researchers successfully identified the Netflix records of known users, uncovering non-public information on their political or even sexual preferences. This illustrates once again that today an individual is not anymore the master of his or her "privacy versus disclosure" balance as it would be the case in a hypothetical silo information system.

The impact of cloud computing

Cloud computing technologies represent another major technological factor which impacts the privacy protection issues. First, these technologies empower Big Data analytics and make available "unlimited" processing and storage capacities to a large number of actors, consumers of personal data or the data controllers. This democratization of computing resources multiplies the personalization opportunities for a larger number of market actors, but it can also lead to more privacy breaches when deriving a commercial value without the user consent. Second, the distributed nature of cloud computing environments introduces additional sources of privacy leaks. Large quantities of privacy-sensitive data are not anymore stored at central servers, but can move across networks of interconnected services and be replicated within multitenant cloud computing infrastructures. Furthermore, the storage and processing resources can be spread across the boundaries of countries and located under the umbrella of different regulations. All these factors create additional uncertainties and risks for the users' privacy.

Privacy versus Personalization dilemma

At the end of the day, instead of being able to tune the Westin's balance, today's end user is confronted with a choice between two extremes, the so-called Privacy versus Personalization dilemma. The user can either choose to expose his personal data in order to take the full benefit of personalised service environments while taking uncontrollable risks regarding his privacy, or he can decide to dissimulate his personal data and refuse the personalization.

Note however, that personal data is the fundamental currency of today's Internet economy. It is a key feature of most of the current services on the Web such as search engines, e-commerce portals, online video portals, location-based services or online social networks. These systems build user profiles based on their consumption activities or interactions with the system, and their business models rely increasingly on the exploitation of personal data through targeted ad and customer attraction or retention. Therefore, the choice done in the Privacy versus Personalization dilemma can have a considerable economic impact.

Although today most users continue by inertia to use the available service offers, the number of privacy-sensitive users keeps growing. So, according to Eurobarometer's 2011 data protection survey, 70% of individuals have had concerns about the use of their personal data. Furthermore, 68% of respondents to Ovum's Consumer Insights Survey said that they would use privacy controls to block the collection and use of their data.[4] This indicates that consumers' distrust of online businesses is deep and persistent, and Internet companies can no longer rely on their inertia regarding privacy.

The scenario of market disruption

These considerations bring us to a scenario of market disruption which can significantly limit the ability of online business actors to continue monetising personal data. This scenario is motivated by the negative consumer behavior with respect to personal data collection, but at the same time it is supported by increasing regulatory constraints that force various OTT service providers, ad networks, search engines, social networks and other data controllers to return the personal data control to the consumer. Thus, the users can at some point prefer their personal data safety and security to the added value of the personalised services. This will result in Big Data pollution with imprecise, noisy, or even misleading information, and significantly reduce the statistical validity of inferences derived by data analytics engines. An important factor for the disruption of the existing *status quo* is the availability of technical means at the disposal of end users preventing the user tracking practices, e.g. cookie auditing tools, personal data traffic monitors, tools for tracking the trackers, etc. Finally, this process is accompanied by the emergence of alternative offers from new incomers in the area of personalised services which adopt a fundamentally different paradigm of privacy-preserving personalization.

The role of telcos

In this challenging context, telcos have a strong card to play by taking the advantage of their comparatively trusted relationship with subscribers. Telcos collect personal data through registration and billing procedures and unlike their OTT rivals, are not entirely reliant on the tracking of personal data to feed

[4] "Personal Data Futures: The Disrupted Ecosystem." OVUM report – TE004000677, Feb. 2013.

targeted advertising. Much of telcos' personal data is collected by permission-based methods and is more accurate, although it is actually underutilised,[5] So, telcos could better leverage their subscriber data while maintaining and enforcing their trusted relationship. To that end, they need to develop more personalised services by breaking down their internal silos. This will improve the customer experience and increase customer stickiness. Furthermore, telcos have the opportunity to take the role of a trusted intermediary between the end user and the other actors of the personal data ecosystem. They can build personal data vaults or identity broker services which give the control of the personal data to their owners (end users) while enabling the operation of the ecosystem. Such solutions need to be heavily supported by privacy-preserving data mining and privacy-preserving personalization technologies.

Privacy-preserving analytics

Privacy-preserving analytics refers to methods which allow exploring the data and exploiting their utility without unveiling the sensitive information. For example, a processing entity that carries out a computation (evaluating a specific function) over some input data should not be able to discover sensitive information contained in the data sources. As we discussed earlier, in the case when the user identification is considered sensitive, simply removing the explicit identifiers from the data sources is not sufficient to ensure that privacy-preserving property.

One of the well-known approaches to this problem is the homomorphic encryption technique, an encryption scheme which allows certain algebraic operations such as addition and/or multiplication to be carried out on the encrypted plaintext, see e.g. below.[6] The sources data are encrypted, with private keys available only to the sources, so that their communication to a function computation entity does not disclose any information. The latter, however, is able to carry out the operation on encrypted inputs and then sends back the results so that each source node can decrypt and discover the correct value of the computed function. These cryptographic techniques are in general heavyweight and imply an important computational overhead which can be an obstacle for practical deployments.

A different direction actively explored in the research community is the approach of statistical perturbation procuring formally provable so-called

[5] "Telcos: Leveraging Trust Through Privacy Management", OVUM report – IT012000074, May 2013.

[6] Daniele Micciancio. "A first glimpse of cryptography's Holy Grail." Commun. ACM 53, 3, p.96, March 2010.

differential privacy guarantees[7]. Here, the approach is different; instead of encrypting the source data, some controlled noise is injected into the original data, so that their utility is still preserved from the perspective of the computed function. The interesting point here is that by tuning the amount of perturbation introduced in the system one can manage the trade-off between the privacy protection and the degree of personalization; the smaller is the noise injected into the original data sources, the higher is the preserved utility, and therefore, the degree of personalization provided by the system. Although this cannot be done at the level of each individual user, this possibility of noise tuning, however, echoes with the desire to establish Westin's balance between privacy and disclosure.

Other conceptually different approaches to privacy-preserving computations develop the paradigm of privacy by distribution. While in these approaches some lightweight encryption is still used, the emphasis is not, however, on encryption schemes, but on data distribution. The idea is to keep the information as local as possible and to apply some intelligence locally in a way that allows making computations at local nodes while accomplishing global tasks and achieving globally coherent results.

Let's take the example of onion-routing techniques used for anonymous communication.[8] Here, a sequence of nodes participate to a message delivery from the source to the destination, but each node knows only its two neighbouring nodes in the global route and is not able to discover the source or the destination of the message, neither it can read the encrypted message itself. In this case, the distributed knowledge of the routing information combined with some basic public key encryption ensures the anonymity of delivered messages.

From a slightly different perspective, various personalization approaches or more generally the data analytics tasks need to compute the similarity between two objects. In a straightforward traditional approach the computing engine accesses to each of the two objects to evaluate a given similarity metrics (i.e. the objects are copied into the same space). This violates the privacy because the objects need to be visible to a third entity. Here, one can take the benefit of locality-sensitive hashing techniques in order to compute the similarity between objects without comparing them explicitly ones to others. This is achieved firstly by broadcasting some randomly generated pivot data to the local nodes. Then, each node can identify its nearest neighbours by

[7] Cynthia Dwork. "Differential privacy." In Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP), 2006.

[8] Roger Dingledine, Nick Mathewson, and Paul Syverson. "TOR: The second generation onion router." In Proc. of USENIX Security Symposium, 2004.

comparing locally to these random pivots, without communicating the local (private) data to a central computing entity.[9]

Last but not the least, when considering the appropriateness of different privacy-enabling technologies, the human factor should not be forgotten. An ideal balance between the desire of communication and that of privacy can only be achieved by considering each individual's need. This means that the user cannot be taken out of the loop just because the service provider employs this or that privacy-preserving tool. Simple opt-in/opt-out choices are in general far from being satisfactory. The user must be assisted in making the most appropriate personal decisions with regard to his privacy, and the underlying privacy protection technology should provide this possibility.

Armen Aghasaryan *is a senior researcher in the Enabling Computing Technologies Research Domain at Alcatel-Lucent Bell Labs in Villarceaux, France. He received an M.Sc. degree in control system engineering from the Yerevan Polytechnic Institute, and M.Sc. degree in industrial engineering from the American University of Armenia. He holds a Ph.D. degree in signal processing and telecommunications from the University of Rennes, France. Before joining Alcatel, he spent two years at France Télécom's research lab in Lannion. In the past, he intensively worked in the area of network management by elaborating new techniques of distributed fault diagnosis and alarm correlation. His current interests include distributed recommender systems and privacy protection technologies. He is a member of Alcatel-Lucent Technical Academy.*

[9] A. Aghasaryan, M. Bouzid, D. Kostadinov, M. Kothari, and A. Nandi. "On the use of LSH for privacy preserving personalization." In Proceeding of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TRUSTCOM), July 2013.

Improve Privacy User Experience to Unleash the Associated Value Creation[1]

Stéphane Lebas

Privacy (h)as value

Companies are already today building models where privacy is seen as a competitive advantage or even as a marketing feature by itself.

A few examples by App.net:

"Our most valuable asset is your trust. Many people have become so cynical about user-hostile, privacy-violating social services that they refuse to participate at all. We can understand why. Earning your trust is the most important thing we can do. It won't be easy, and we will make some mistakes, but we will do our best to be honest and transparent."

"You own your content. Everything that you put into App.net is yours. That means we'll never sell your posts, private messages, photos, files, feed, clicks, or anything else to advertisers. You'll always be able to easily back-up, export, or delete all of your data."

"We are selling our product, NOT our users. We will never sell your personal data, content, feed, interests, clicks, or anything else to advertisers. We promise."

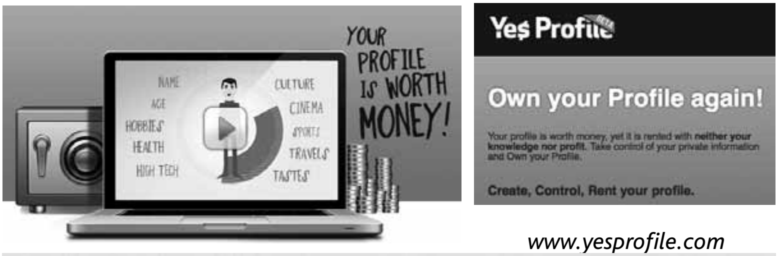
These service providers tend to criticise others, which are less user-privacy friendly.

From my perspective such an approach is not efficient: The question here is not to complain about competition, not even to evaluate privacy risks and user protection, the question really is to think about privacy in terms of value creation.

[1] Transcription of the speech given during the Privacy seminar of Institut Mines-Télécom.

One of the key concerns comes from the fact that the best way to create value is to share value, and to share it of course with end users. There is a lot of value in personal information and Big Data, but to start to unleash this value, you need to share it.

To go further in that direction, we can identify some startups that even promote "Privacy + Data Monetisation" services:

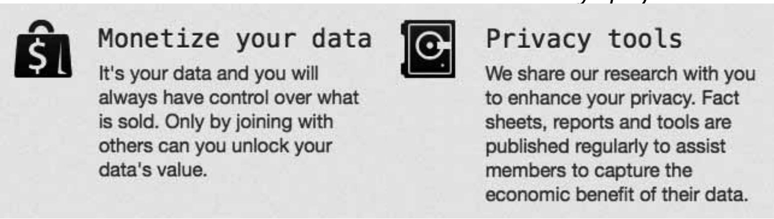


Own your Profile again!

Your profile is worth money, yet it is rented with **neither your knowledge nor profit**. Take control of your private information and Own your Profile.

Create, Control, Rent your profile.

www.yesprofile.com



Monetize your data

It's your data and you will always have control over what is sold. Only by joining with others can you unlock your data's value.

Privacy tools

We share our research with you to enhance your privacy. Fact sheets, reports and tools are published regularly to assist members to capture the economic benefit of their data.

www.moneyformydata.com

In both examples above, there is a mixed claim between monetising your data and using privacy tools. They both present privacy in the same way: a safe repository box. The best way to share the value, in their perspective, is to share the associated money generated by customer data.

I think maybe the monetary angle is not the best way to convince people to share their personal data. It might be better to rely on other benefits for the end users, on other value propositions.

These companies claim that you can register and fill in your personal data, that you will be able to manage your personal data and get money from it. So, your personal data is supposed to be safe and private. But they didn't forget to add a few buttons for you to publish the value of your data on the social networks – which is paradoxal...

How corporations comply with the regulation

When we look at large corporations or mass market services, we have to admit that many of them are just implementing very basic sets of privacy features and requirements.

It is usually limited to cookie management, to "opt-in / opt-out" options and to display on the website of privacy policy.

There are a lot of solution and service providers who help large companies to comply with the 2009 amendments to the E-Privacy Directive (Cookie Directive).

One example:

TRUSTed Consent Manager is a leading solution in the EU that:

- Provides brand protection by reducing regulatory compliance risks
- Ensures transparency for consumers through clear notice and choice regarding the collection and use of their personal information
- Implements easily into a publisher or website operator

www.truste.com

But even so, the question remains the same: How do I minimise the impact of these requirements on the customer's experience? By having a very small privacy section, putting the opt-out button in an hidden place... The question really is to switch from "what is the impact on the user experience" to "what could be the benefit in terms of user experience."

Large corporations need to see privacy not only as something they have to comply with but in terms of benefits.

It could be seen also as a way to avoid the debate around sharing the value; maybe they have to focus on user experience. Not just on recommendations, but on helping users to understand what they really are doing on the Internet and on allowing them to enjoy a safe navigation.

Privacy's paradox

From the user-centric perspective, customer privacy meets an unexpected paradox: When you ask Internet users: "Do you feel that your personal information, reputation and privacy are at risk on the Internet today?" 90% of respondents answer Yes.

Of course, it is not people's first concern.

For 56% of users, they themselves should be responsible for managing and guarding online privacy.

46% of people only answer that private companies that store data (social networking sites, databases, blog platforms, etc.) should be responsible for privacy (Source: 123people online customer survey 2011).

BUT: to use a smartphone or download an app, absolutely everyone validates "Terms & Conditions" with privacy concerns without reading it...

Another study says that 50% users never once in their life read "Terms & Conditions."

If you would like to have a clear demonstration of that, you can read all the "Terms & Conditions" you have to accept in order to use your mobile device…

If you look at what you allow Twitter to do on your Android device, it is scaring: They're allowed to have your location (GPS and network), to modify or delete contents from your mass storage, to have access to your network connections – full access – to modify your call logs, to see your contact details, to modify your contact details, and so on.

The truth is that today most people just don't care when they validate such terms and conditions, so our job is to be able to convince the end user and the service provider that there is value in changing such a situation

At the end of the day, it is mainly a question of user experience: When I want to download an app, I want a direct download, I don't want to read terms and conditions. It is the same thing when I activate my smartphone.

Today, service providers and handset manufacturers are using user experience against privacy regulations. We should definitely reverse such situation.

Telco and e-commerce: the YouConnect case

Here is a real trial example of personal data exposition we did with Alcatel-Lucent, Orange and Bouygues, compliant with privacy guidelines and with benefits for everyone. It was an attempt to find a good mix between privacy and value creation.

We started with a business question: The figures are not fully accurate but we can say that at the moment, for some e-commerce services, 30% of new customers acquisition is done directly through the mobile phone. People discover the services on their mobile phone. It represents 10% of revenue, but if we look in detail, only 30% of people who download the app go to the end of the registration process. Because it is very painful, you have to put in your name, address, full name, date of birth, email address, pass code, etc. The business question is: "How to boost registration rate for e-commerce on applications on smartphones." A really interresting question.

What we did in France, what we called the "YouConnect trial," was a way to allow the application to automatically get all the personal data information, to complete the registration process very quickly. Basically, you ask to register, then, on the registration form, you just have three clicks to acknowledge the use of your data from your mobile operator (name, forename, date of birth, email address, postal address, landline phone number, mobile phone number, gender).

Telco doesn't send the data to the service provider, it just sends the data to the application, locally, and until the customer modifies and validates his data or acknowledges the data, he his totally in control of his data. After three clicks of customer consent the data is transmitted to the service provider. The user is really in the middle of the relationship between the third party and telco, and he has full control over his privacy and the content of the data (he can modify it).

From a technical perspective, the pilot was based on an open API approach, "Code is law" approach, open authentification mechanism. It was of course fully compliant with French regulations.

To conclude, here are three recommandations to unleash the value of privacy features:

– Have better leverage on user experience to educate customers on privacy on the one hand, and on the benefits of data sharing on the other hand.

– Give back control and value to the customers in order to onboard them.

– Maybe use any massive security and privacy breach in the coming years as a tipping point? This may be the only solution for mass market users to become fully aware that privacy is a critical concerns for everyone.

Stéphane Lebas *is Product Marketing Director in charge of Applications and Smartphone Services within SFR. He has been working for many years on Location Based Services and API exposure to third party with a focus on Privacy and Customer Data Management. Since 2010, he has also been building new activities around SFR network Big Data analytics.*

The Future of Privacy Concerning the Financial Services: From Physical Vaults and Bank Secrecy to Data Leverage and Digital Literacy?

Matthieu Soulé

Banking and insurance activities: a brief introduction

The development of financial services has always been directly correlated with the development of the needs of societies and economies to build and grow cities, businesses and trade.[1] On the one hand, a bank's role is to connect the money from those with surplus capital to those with capital deficits, and consequently allocate the financial resources in an optimal way. On the other hand, insurance is a mechanism to transfer the risk of a loss from one entity to another in exchange for payment.

The state of the financial system as a network of economic agents (both individuals and companies) is a sign of the vitality of an economy and a mirror of the trust inherited by the values supported by the society. The financial services sector is one of the key actors of the global economy as it helps to raise the virtuous circle of trust. As a third party they allow trade and transactions to take place between people in different locations who do not necessarily know each other.

[1] Noble Foster Hoggson, *Banking Through the Ages*, 1926.

"Keep the money safe"

From an individual perspective, the primary role of a bank is to "keep the money safe," either in a physical vault, or more recently in both physical and electronic formats. On the other side, also from an individual standpoint, insurance is there to "protect people and goods against life hazards."

Insurance and banking activities are thus based upon a high level of trust and long term relationships because of the very specific nature of these businesses related to the protection, wealth and financial life of their clients. For centuries the interactions with the bank have been developed upon the direct relationship between the clients and their relationship manager, or advisor, even if today this is extended by the digital tools at clients' disposal.

Last but not least, something quite specific to banking is "bank secrecy": One of the conditions of the relationship between a bank and its customer is that information about clients and their affairs are treated as strictly confidential and are managed under professional secrecy acts. Like doctors or lawyers, the bank cannot share information about individuals and their financial information, whether they are clients or not. Depending on the geography, there are some exceptions to this rule such as tax evasion, funding terrorism and money-laundering activities (take as an example Tracfin in France, which is the governing body for the Ministry of Economy and Finance to track money-laundering and terrorism activities[2]).

Regarding personal data and other forms of data managed by banks and insurance companies, within each geography both are compliant with the national laws in place and are supervised by both the data protection authority, where present, and the financial sector regulator. In France, for

[2] www.economie.gouv.fr/tracfin/accueil-tracfin.

example, the Commission Nationale de l'Informatique et des Libertés (CNIL)[3] is the data protection authority, and the Banque de France with its body the Autorité de Contrôle Prudentiel et de Résolution (ACPR) supervises both banks and insurance companies.[4]

BNP Paribas: Digital as an opportunity to redefine and enhance the customer relationship

After introducing some key elements for the financial services activities, I would like to provide some information about BNP Paribas and explain why the evolution of privacy is essential for us in a more and more digitally-influenced environment for the financial services sector.

BNP Paribas is one of the leading financial services companies in Europe with 25 million retail banking customers in 40 countries and 283,000 corporate customers. The retail banking activities represented 61% of BNP Paribas' revenues in 2013, and if you add the other retail activities from insurance to consumer credit and car leasing, BNP Paribas manages a lot of complex data for both its clients and its own purposes, from ratio calculation to risk assessment to service delivering.

The retail banking business (banking to individuals and companies) is all about personal relationships with the clients, helping them attain good financial health and supporting them to successfully achieve their goals. Today in a bank like BNP Paribas, retail banking represents a headcount of 142,000, largely client-facing with more than 150 business centres across Europe and 7,300 branches worldwide for 24.4B euros in revenue in 2012. The business of a bank is to financially help their clients with their life projects, such as setting-up their businesses, buying their house, their first car or saving money for their children's education and future.

The bank is progressively shifting within this new digital environment, following its clients: there is a multiplication of the interactions between the banks and the customer, and consequently a multiplication of data collected from customers that can be used to better serve them. For example, the total number of contacts with clients in the developed countries has been multiplied by two for retail banking between 2004 and 2012. It started from a base of 95% of contacts made by traditional channels (branches, ATMs and call centres) in 2004 to 46% in 2012, which means that digital channels (mobile and online), with 54% of the total of interactions, are now the first channels

[3] www.cnil.fr.
[4] www.acpr.banque-france.fr

of interaction between the banks and their customers,[5] and this also intensifies the relationships with their clients. As the total number of interactions doubled almost entirely because of these new channels, when people come to branches or have a call with their relationship manager, they expect a higher quality of advice and therefore, it improves the quality of the relationship with their advisor.

Parallel to this, from the usage of the electronic card to the categorization of expenses and the use of digital applications that have been developed in the last few years, there is an explosion of data creation within retail banking activities derived from client usage which could be leveraged in a win-win configuration. The same will happen soon for insurance activities on a larger scale with the emergence of new measurements from sensors installed in cars, at home, to mobile health trackers which will allow the launch of new services and offers to individuals and corporations, thanks to the intensive usage of data collection and analyses.

From data collection to data leverage: First experimenting new value-added services for individuals, secondly monetising the service

Banks today could be seen as giant technological actors with their data centres which manage billions of transactions a day, and millions of "customer events," from cash-withdrawals to account statement viewing on a mobile app, and the massive information networks formed by these economic actors. I like to say that at the macro-level, a large bank such as BNP Paribas is the equivalent of an almost real-time INSEE (the French national statistic and economic studies agency): Its clients represent a very good sample of economic agents in France and in Europe. Their economic decisions are reflected and captured by their transactions, such as credit, investment and deposit.

At the micro-level, when an individual uses the bank to host his main account, the bank is able to identify the sources of income, large categories of expenditure and the economic links between other individuals and businesses. The issue for a bank is not to use this data in an inappropriate manner from the client's, and also the regulator's, points of view.

The new possibilities of leveraging this data for new services and products are phenomenal: From individual to corporate services, the usage and combination of data are undoubtedly a great source of the future innovations that will take place in the financial services sector.

[5] BNP Paribas presentation, Barclays Conference, New York, September 2013.

As a concrete example of the use of financial services data for non-financial activities, Bundle.com is a service which has been co-developed in the USA by Citibank, Microsoft and MorningStar (provider of financial information) and was launched in 2010 with the ambition to create a "personal finance social-media site that will change the way people discuss saving and spending money."[6] One of the actual live beta tests is marketed as "bundle – unbiased, data-driven ratings" using data from literally billions of anonymised Citibank customer card transactions to identify a certain number of interesting insights in cities. An example of this is the catering industry in New York (LaFourchette.com meets transaction data)[7] collecting observations such as: real average bill paid by people, which days people go to the restaurant, neighbourhood of origin of the people coming to the restaurant, in which other restaurants these clients regularly eat… The service is still in its beta phase but this illustrates how data from card transactions could be leveraged to collect information and identify patterns about the restaurant businesses, and even advise new set-ups based upon this market data.

Another example was a startup called BillShrink.com[8] which was created in 2007 with the aim of "providing a free, online service to help consumers make better purchase decisions for complex product categories." As an individual, you were providing key information about the type of consumption habits you had, for example from your phone bill (the price you paid, number of minuts, sms…), and Billshrink.com would propose counter-offers based upon your own declarations. The service pivoted to become Truaxis and was finally acquired by MasterCard in 2012.[9] Mint.com would go even further: from an aggregation service of your different banking accounts and by obtaining details of your transactions through the use of your login and passwords to access your different accounts, they announced that they would make you counter-offers directly based upon your transaction data. This did not happen as Mint.com was acquired by Intuit in 2009 before really having the opportunity to test the idea.[10]

[6] "Citigroup, Microsoft and Morningstar Launch Bundle.com – a new social media site", Jacksonville, 21st Jan 2010.

[7] http://bundle.com/guide/city/new-york-ny/restaurants.

[8] http://www.billshrink.com

[9] "MasterCard Acquires Truaxis, Inc. to Enhance Delivery of Personalized Shopping Offers and Rewards to Consumers", Press Release Mastercard, September 6, 2012.

[10] History of Mint.com: http://en.wikipedia.org/wiki/Mint.com.

Data collection and analysis in exchange for personalization and customised experience: Is the trade-off for data privacy really that easy?

The biggest fear for all these new digital services exploiting personal data is to go too far, as in the case of Target in the USA in 2012 with their loyalty programme, when a father heard about the potential pregnancy of his daughter before she told him, as she used his loyalty card to make a purchase and he consequently received offers for babycare products from Target.[11]

In another sector, entertainment, Disney implemented a giant $1B project called "My Magic Band" which has been in pilot for two years in Florida: You receive a band (bracelet) before going to the Theme Park, which is essentially a digital wallet which stores your hotel room key, your entrance ticket and your money. This service allows you to "enjoy the magic world of Disney with this frictionless process."

In the words of the Disney CEO and CFO in different conferences in 2013: "Now there is a lot more that comes with it, customization and personalization. It enables us to know who you are and essentially enables not only you to tailor the experience that works best for you, but also us to help you do that; that is a big deal. The wristband also is your room key, it is your ticket, it is your entrance to these attractions that you reserved. [...] However, a secondary driver of revenue will be the services that we can now offer on a personalised basis because we know who you are, where you are and, if you tell us, why you are coming to Walt Disney World for this vacation, whether you are a first-time visitor, a 50th-time visitor, it is your child's fifth birthday, it is a graduation, it is an anniversary. The more you share with us as a guest the more we are able to tailor services and, we think, get a lift in selling those services. So that is the fundamental economics."[12]

In our digital era, the equation for privacy is above all a question of what kind of positive aspects can be seen from the collection and analysis of personal data in the future.

For me, as long as data derived from human behaviors is concerned, there are unlimited possibilities to restitute this data to consumers and create a new level of awareness for them, helping them better manage their lives. It is true for banking, health, energy consumption and education. The more tools you can give out to empower people and better inform them about what they care about, the more comfortable they will be with their data being used.

[11] http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did.

[12] Disney CFO, Bank of America Merrill Lynch 2013 conference & Disney CEO – Goldman Sachs Conference - September 24, 2013.

They are also susceptible of requesting more of such services even if they have to share more information and personal data in the process.

Of course there is the question of technical feasibility in terms of confidentiality, analysis and data-rendering. The personal authentication and data reliability are pre-requisites for the correct use of personal data in a manner that benefits both the individual and the business which is providing the service. For example, in the banking industry, there is a strict regulation regarding the account opening process (Know Your Customer procedures, KYC) and suspicious transactions: You need to ensure that reliable data, or a set of proofs, are collected to guarantee the correct level of customer service.

There is also a real question about which kind of third parties can be trusted today in the context of the Snowden revelations, both about governments and technology giants. Some forces would probably push in favor of more independent data vaults. Also likely to emerge are new forms of protection equivalent to the so-called "electronic vault" to avoid data loss, and also to avoid this data being seen by, or compromised by, corporations or governments.

The concept of Vendor Relationship Management (VRM, as opposed to CRM, Customer Relationship Management), presented in the book *The Intention Economy – When Customers Take Charge* written by Doc Searls,[13] is probably one of the most advanced visions on the subject, and is becoming more and more relevant in a context where new independent third parties will have to be created. The idea is to develop tools that help people take better decisions regarding their service providers and manage their relationship. The tools could be used to make some Request For Proposal (RFP) for services and invert the bargaining power between corporations and individuals.

Value creation derived from data in the digital era: A combination and positive externalities

The new "personal data" paradigm is about the new possibilities of data combinations and the possibility of comparing these to a pool of defined data sets. Value can be created both for the producer of the data and its ecosystem.

At L'Atelier we recently published a prospective study for the Forum d'Avignon 2013 entitled "Big Data, Big Culture? The Growing Power of Data and its Outlook for the Economy of Culture."[14] In this study, we developed in detail some of the strategies of key Internet powerhouses such as Netflix, Pandora or Zynga, regarding the collection and analysis of large sets of

[13] http://www.searls.com.

[14] http://www.forum-avignon.org/fr/publications#3187.

personal data, like movie ratings, that will become a standard for the creative industries.

We also took as a specific example the interest in experimenting some ideas to carry out cross-fertilization of data collection and analyses between culture and tourism industries in partnership with private actors: In the summer of 2012, the Côte d'Azur Regional Tourism Committee (CRT) and the telecommunications operator Orange conducted a pilot experiment intended, firstly, to quantify and model the presence and movements of visitors in the Côte d'Azur region using data collected from their mobile phones, and secondly, to extract the meaning hidden in this data to facilitate and industrialise decision making in managing the tourism offer in the region. Each year, nearly 77 million foreign tourists visit France. The "tourist audience" on French soil contains growth opportunities worthy of the digital economy. For example, the audience visiting from the BRICS countries is experiencing a double-digit growth. Tourism in France affects about one million jobs directly and almost as many jobs indirectly. In 2012, it generated consumption of nearly 138 billion euros, equivalent to 7% of the French GDP. Given these figures and the natural proximity of the two sectors, it is legitimate for the cultural industries to draw upon Big Data initiatives that have already been implemented for tourism, and to consider potential economic synergies based upon shared use of data. In both these industries, it is personal data that has been anonymised and aggregated which provides them with real added-value, allowing them to take better decisions for investment and their respective offers to the public.

From absolute consent to dynamic consent: Create the check-and-balance of the digital dge

There are real economic and social values in cross-referencing data. But this has to be done with consent and what I call "dynamic consent." You always have to carry out a check and balance in order to protect individuals from data-mixing and abusive use of data. This means going back to the dilemma between opt-in and opt-out regarding data protection: There is a need to make the consent process frictionless, and also to allow the person to remove their own data whenever they do not feel comfortable.

One of the best ways to do this could be by businesses adopting a proactive approach to give clients back access to the data concerning them. It has been on the agenda of the UK government for a few years with the Midata project, led by the Bureau for Business, Innovation and Skills. The Midata project is working with businesses to give consumers better access to the electronic personal data companies hold about them. It also aims at giving consumers greater control of their own data. "Giving people greater access to electronic records of their past buying and spending habits can help them to make better buying choices. For example, data that a phone company holds about your mobile use may help you choose a new tariff."[15] Some of the UK's biggest companies which are already working on the project include Google, British Gas, Lloyds TSB and O2.

From an individual point of view, the issue about personal data is that you have to experiment the real value of a certain set of data you are willing to share with someone, and to do this you need to be ready to give away a little of your privacy. But you want to be in control and have the possibilities to cancel or opt-out of this sharing phase; to be sure it is not definitive. One extreme example is that of medical records: I am ready to share my medical data with professionals and online services that I trust, but not with corporations that could use it at my expense (car insurance for driving behavior, medical conditions...).

This question of trust is a key element and must be understood in a dynamic context: as a corporation, you can betray individuals once but they will no longer trust you, and a lot of the trade-offs about them are in collecting new data and actions which will occur in the future. Individuals are not giving access to an unlimited gold mine, and they have to be treated with respect, which is good news: The value is more and more in the future data which an individual will share with the services rather than the stock of information that the service has on him (flow > stock). And for one specific reason: If they want to better serve you in the future, businesses have to earn your trust and they cannot abuse it. If this is not the case, you can unsubscribe from their services and go to see a competitor which will potentially take better care of you.

Need for digital and privacy literacy: The analogy with financial literacy

The gate-keepers for individuals will be the trust they have in the institution they are giving or sharing their data with, as well as the atmosphere of transparency regarding its use. There will be a need to implement appropriate tools regarding / securing privacy to let people know what you are doing with their data and how it is benefiting them.

As with the use of new means of payment, there is a need for educating people and giving them tools to be in control. The first time you used a debit card, you may have been likely to make a small cash withdrawal or pay a small

[15] https://www.gov.uk/government/policies/providing-better-information-and-protection-for-consumers/supporting-pages/personal-data

amount at your favorite store. After you tried it several times, and became confident that it was convenient and secure, you ended up trusting the system because it did not let you down. This is what creating a virtuous circle of trust is: The more you use it, the more confident you are and the more you want to use it in the future. Like for credit, the regulator will probably have to incentivise the private sector to educate their public, and also to take a commitment regarding the lisibility / transparency of the terms and conditions of the services they provide. For example, according to the financial regulations in France, you have to protect the individuals against "themselves" when they make an investment; the bank has to confirm the client has the capacity to understand the risk they are taking.

Raising the level of understanding about privacy and personal data will be necessary to avoid major scandals and maintain people's trust in digital services as they become more and more sophisticated in terms of usage of personal data. The journey is just beginning…

Matthieu Soulé *is a strategic analyst at L'Atelier BNP Paribas. He graduated from the Audencia Nantes Business School with a Master in Management, and has been working within different innovation centres for the BNP Paribas Group, of which the Atelier North America in San Francisco and the Center for Innovation, Technologies & Consulting (CITC) in Paris. He is also the Vice-President in charge of the organisation Finance for Youth Diplomacy (www.youth-diplomacy.org). He is a regular contributor to the programmes proposed by the Fondation Télécom including "Privacy" and "New Business Models in the Digital Era."*

An Economist's Thoughts on the Future of Privacy

Patrick Waelbroeck

Introduction

Privacy deals with personal information that identifies the preferences of a person. The identity of the person is not so important in economics. In fact in the neoclassical equilibrium model, consumers are anonymous and have no identity, and what they do is interact with each other. The identity of a person plays a role only if it influences his or her choice. For example, it is easier to give to family and close friends or to people who share certain beliefs than to strangers. Akerlof and Kranton (2000) discuss this notion of identity. However, the choices that we make are important because they reveal our preferences. This is known as the axiom of revealed preference in economic theory. So all our online activities, our choice of websites to visit, the comments we post, our online purchases, our posts on Twitter can be considered as personal information because they reveal our preferences and our willingness to pay for a product or a service. This is the reason why Big Data technologies combine as many separate datasets as possible in order to gain the most precise knowledge of our online profiles.

We receive information filtered by "infomediaries" and platforms such as Google or Amazon. For example, Google search engine filters search results based on a person's geo-localisation, browsing history and profile. Amazon runs algorithms to deliver customised product recommendations based on a person's browsing history and purchases. These filters raise important economic questions that I will discuss in Section 2.

We also produce personal data that have a commercial value. We leave traces and footprints unintentionally but we voluntary contribute to online communities such as eBay, Amazon, Wikipedia, Twitter, YouTube. I discuss the economics of contributions and of online participation in Section 3. Privacy laws should not forget that Internet users want to express and publish themselves online.

Digital identities are masks that we wear online to distort our identity. These masks are email addresses, avatars in online games, pseudonyms used in discussion forums or to visit online dating sites. There are two opposing views on digital identities in the sociological literature. The first assumes that people use Internet tools to build their identity: They use avatars and adopt behaviors that are different from their real personality. These digital identities depend on the technological, social and cultural context. Digital communication tools represent a form of laboratory to build and test alternative identities. The second view considers that Internet users present themselves online as they are in real life, but that they actively manage what they disclose to other members of their communities. The Internet user blurs his or her identity by using anonymization tools, by withholding information or by giving misleading statements. Both approaches are not necessarily contradictory, as users move from one to the other in a dynamic process involving self-construction and self-projection.

The fact that Internet users mask their identities greatly limits the extent of price discrimination and targeting. Thus, the active management of digital identities challenges the metaphor of the onion, which postulates that a person's identity consists of different layers left by past socio-cultural influences. According to this view, efficient targeting needs to peel the successive layers to get to the core of a person's identity. Hui and Png (2006) review the literature on the economics of privacy and price discrimination. It turns out that these different degrees of anonymity are also important for understanding participation and contribution to online communities because a member of a forum on health problems does not contribute the same way when he is anonymous and when he is not.

1. Filters, masks and the limits of Big Data

1.1. Algorithms, freedom of choice and competition

Information filters that I have discussed above are sometimes called algorithmic regulation since they condition our behavior. They raise important economic issues mainly related to competition law. Indeed, how can we ensure that consumers do not miss opportunities and that these filters do not reduce competition by excluding certain content, products or services? Who will guarantee that privacy protection tools will be offered to consumers?

1.2. Sample selection

Individuals may document false identities or partial identities online or remain anonymous. In addition, they can contribute actively or not at all to online communities (open source, wikis, forums and other knowledge communities). Therefore, certain demographic data and opinions will be over-represented, thus creating a selection bias in the statistical analysis of these datasets. Selection bias is also an issue when there is a market for reputation, where agents sell a rating. One can buy "followers" on Twitter or "Likes" on Facebook. More generally, Big Data correctly anticipate the behavior of individuals if they are relatively passive. On the contrary, when individuals anticipate the rules that are applied to them, they can manipulate their personal data to make the algorithm inefficient.

1.3. Authenticity

"Is everybody happy on the Internet?" 99 percent of faces that you see on the Internet represent people smiling. When you scan personal ads on online dating sites you will find out that all male users make more money than their peers. These are lies and Big Data technologies need to test the reliability of the datasets being used. Tripadvisor is employing 100 persons full-time to filter out questionable comments. What are the consequences of a firm or government applying an algorithm to you based on incorrect information? Authors such as Crawford and Shultz (2013) have strongly argued for a technological due process to uncover the algorithmic rules that are applied to us online. But if Internet users know the algorithm that is applied to them, they can again manipulate the algorithm and Big Data technologies become less efficient (see the discussion in the previous subsection).

2. The Internet user as a producer of information

Connected health devices such as Withings devices can measure your weight, blood, heart rate, and sleep cycles. These connected objects allow you to share personal health data and contribute to databases that aggregate data from all users. But why share sensitive personal data? Why contribute to this common knowledge base? One can think of the following reasons: To better know oneself by measuring and comparing our personal data to the rest of the community in a quantified self programme, for instance, to contribute to a database on special illnesses, to stay motivated during a diet. More generally, there are many reasons to contribute and to participate to online communities including: A sense of satisfaction from helping others (warm glow), reciprocity on eBay when a seller rates a buyer (expecting the same in return), career or reputation concern in an open-source project, customization and personal recommendations on Amazon, a sense of belonging to a community, a sense of justice by correcting statements written in an online newspaper (efficacy or self-esteem).

There are thus many private incentives to contribute to online communities that economists have long ignored. The main reason for this lack of interest is the following: Users are asked to contribute to knowledge communities, and knowledge has very specific economic characteristics; it is considered a collective good sharing two properties: It is non-rival and non-excludable; under these conditions, there is underinvestment by private agents. This is also true for online participation. We know for example that 50% of eBay users do not rate people with whom they made a transaction. On Wikipedia, people talk about the 90-9-1 rule: 90% of community members are lurkers, free riders or have opportunistic behavior and do not participate actively in the development of the knowledge base; 9% update existing pages; 1% creates original content. The intensity of participation thus varies widely in the community.

What is the economic value generated by these contributions? I think that economists have underestimated the role of individual contributions on the success of large Internet firms. Indeed, individual contributions are at the origin of the development of companies such as Amazon that guides its customers through product ratings left by other customers. EBay has reduced information asymmetries using an online reputation system built from customer feedback. YouTube could not exist without user generated content. This creates a paradox. If individual contributions are so important for the development of online businesses, why are individual contributors and active participants not directly paid for their services? Indeed, most of these services are free to users, but in return they are not paid for their contributions. Some industry observers speak of free digital labour, others of slavery. We are in some sort of a barter economy where contributions and personal information are exchanged against a service.

3. The future of privacy

The paradox of data protection. There is a fundamental trade-off between the economic value of personal data and their degree of anonymity. This trade-off is amplified by the development of Big Data technologies that allow firms to connect previously independent datasets. Too much protection reduces the economic value of personal data and could lead to a paradox where data protection offices around the world battle to protect anonymous data that have no value.

Privacy and power. New information processing technologies will give more power to consumers and citizens but also more power to governments and states. Designing privacy laws that maintain the balance of power between citizens and governments is a big challenge for democracies in the future. On the one hand, consumers will be better informed and make better decisions by using new tools to process massive data. Open data will enable citizens to better assess public policies. They will gain autonomy and the democratic process could be reinforced. At the individual level, new connected devices will better monitor health, prevent illnesses and contribute to personal happiness. On the other hand, traces and footprints left voluntarily or involuntarily on the Internet make it easier to monitor deviations from the mean. This can be used by unethical firms to manipulate consumers using human weaknesses pointed out by behavioral economics (Calo, 2013) or by a central authority wanting to strengthen its political power by harassing minorities and stigmatizing unwanted behaviors.

Privacy and innovation. When designing privacy policies, we should not forget that future business models and innovation will greatly depend on personal information. We should discuss privacy and innovation policies at the same time. The question that will need to be answered is where to set the cursor between protection and innovation.

Privacy and competition policy. There are many upcoming challenges related to competition policy, as I have already discussed. New privacy laws need to make sure that privacy protection tools will be competitively supplied on the market, that search algorithms do not leave potential competitors out of the market and that Big Data algorithms do not leave consumers with a limited set of choices.

How to share the value generated by personal information? Perhaps the biggest privacy challenge is to find a way to better share the value generated by personal data and contributions. Current discussions have focused on market for personal data, new tax regimes on value added generated from personal contributions, and universal wage.

Autonomous data, licences and Digital Rights Management (DRM). Internet users could licence their personal data for different uses by different companies. The licences could be enforced by DRMs or privacy by design. Data could become more autonomous, fueling innovation while respecting individual rights.

Patrick Waelbroeck *earned a Ph.D. in economics from the University of Paris 1 Panthéon-Sorbonne. He also holds a master degree from Yale University for which he obtained a Fulbright scholarship. His research focuses on the economics of innovation, the economics of intellectual property, Internet economics and the economics of personal data. Patrick Waelbroeck is a member of the editorial board of the* Journal of Cultural Economics. *He has published widely cited articles on the subject of piracy in the cultural industries, which have influenced the public debate in France, Europe and*

the United States. He is currently president of the international association European Policy for Intellectual Property. Patrick Waelbroeck is also a founding member of the Chair "Valeurs et Politiques des Informations Personnelles" (Institut Mines-Télécom) that addresses legal, economic, technical and philosophical issues related to personal data.

References

Akerlof, G.A.; Kranton, R.E. 2000. "Economics and Identity", *Quarterly Journal of Economics*, Vol. 115 (3). p. 715-753.

Crawford, K.; Schulz J. 2013. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", New York School of Law, Law & Economics Research Working Paper 13-36.

Hui, K.L.; Png, I.P.L. 2006. "The economics of privacy", *Economics and Information Systems*, Hendershott, T. (ed.). Handbooks in Information Systems, vol. 1, Chapter 9. Elsevier

Calo R. 2013, "Digital Market Manipulation", University of Washington School of Law Legal Studies, Research Paper no. 2013-27.

Conclusion: Raising Awareness Around the Concept of Privacy

Carine Dartiguepeyrou

To close the day's programme, let's share a few questions I think still remain and which could be interesting in the future to carry on with the research.

The first question relates to the level of consciousness and the awareness on the issues of privacy, a question I have that came to me after all these days and a couple of months of work: Do we have to wait for problems to occur to do something? How could we basically raise the level of consciousness around privacy issues?

The second set of questions relates to technology solutions, which are very complex and very expensive. The question is, often in the absence of law, how can we push innovation, how can we develop trial and tests, how can we experiment even before regulation takes place? All along this question arose. It is a very important point, that was well put into context by Florence Raynal of the CNIL and Thibaut Kleiner of the European Commission. Having the right to "safely" test and experiment is a key issue and a question for the future.

Another question is legal issues and governance. The speakers share their hopes regarding the move towards more "coregulation" and interdependence, i.e. convergence and minimum standard but not full global harmonisation. Although consensus is currently being reaffirmed, there is still some difference between the approaches of the Organisation for Economic Co-operation and Development, the Council of Europe, the European Union and the Asia-Pacific Economic Cooperation, as Claire Levallois-Barth showed. Regulation often arrives too late when ethical stakes are raised.

By looking at the broader view, i.e. governance and not only legal issues, we tried to capture factors that can be and need to be anticipated. Organising neutral discussion between actors (civil society, companies, public institutions) as well as developing relationships and sharing visions and solutions between public institutions are an essential step of the governance in the coming ten years.

The fourth set of questions refers to social and public value of privacy, which probably is a key subject for the future. The debate is on who should provide these values with regards to public value and social value: Should it come from the private sector, public actors? Should it be regulated, at which point, and by who?

There is still a debate between the different visions of privacy: American vs European, legal paradigm vs business paradigm, citizen protection against intrusion, as with the Snowden case which was mentioned several times during our conference, etc. There is still room, especially in the economic sphere as value creation and new business models are looking for new inspirations in the field of political economy. Social value, open source and innovation are forcing economic actors to reinvent themselves.

Thanks to Helen Nissembaum, we learned that personal data needs also to be taken into its social context. Thanks to Bregham Dalgliesh, we touched upon the possible alternative representation of the dominant Western concept privacy by the Japanese culture.

Beyond even privacy, it shows that public space and surveillance reinforce the perception of globalisation of Westernisation and that it is important to enlarge the subject not only to "the nature of the individual."

The challenge for our society is to move beyond globalisation with a more balanced respect and more effective integration of cultural diversity. Many challenges facing our societies such as the digital transformation, ecological transition and knowledge access require inventing new forms of cooperation.

In conclusion, privacy does matter. It is probably one of the most important ethical subject in the coming ten years. Private companies are taking risks developing new technologies and services in that field. Dominant digital actors are investing in this sphere with very little attention from public actors and civil society. Awareness has to raise substantially so civil society can benefit the most from privacy protection. We hope that this book will have contributed to this awareness.

The conferences of the 17 October seminar are available on : http://www.fondation-telecom.org/actualites/the-futur-of-privacy-retrouvez-les-videos-du-seminaire-177/

Acknowledgements

Many thanks to:
Francis Jutand, Scientific Director of Institut Mines-Télécom,
Véronique Deborde, Directrice déléguée of Fondation Télécom,
Claire Levallois-Barth for having invited Florence Raynal and Winston Maxwell,
Pierre-Antoine Chardel for having invited Helen Nissenbaum and Bregham Dalgliesh,
The partners of Fondation Télécom and of Think Tank Futur Numérique,
Every contributor to this *Cahier*,
Anne Andrault for typesetting and proofreading this *Cahier*,
Nicolas Basset for the layout of the *Cahiers de Prospective* covers.

MINES TELECOM

INSTITUT
Mines-Télécom

The mission of the Cahiers de Prospective by the Think Tank Futur Numérique is to enlarge the temporal horizons of the reflexion on the digital transformation. The Cahiers seek to deal with various themes in a decompartmentalized and transdisciplinary manner by associating the contributions of praticians, leaders, managers, researchers, experts and partners of the Institut Mines-Télécom and of the Fondation Télécom.

www.fondation-telecom.org
www.mines-telecom.fr

ISBN 978-2-915618-25-9