scripted

Volume 12, Issue 1, June 2015

CONTROL OVER PERSONAL DATA: TRUE REMEDY OR FAIRY TALE?

Christophe Lazaro[*] *& Daniel Le Métayer*[*]

Abstract

More than ever the notion of control plays a pivotal and pervasive role in the discourses of privacy and data protection. Privacy scholarship and regulators propose to increase individual control over personal information as the ultimate prescriptive solution to tackle the issues raised by emergent data processing technologies. Conceived as "the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others", the notion of control is not new. It is often considered as the unique means of empowerment of the data subject. The mechanisms of this empowerment remain however surprisingly vague and understudied. What does it really mean to be in control of one's data in the context of contemporary socio-technical environments and practices? What are the characteristics, purposes and potential limits of such control and how can we guarantee data subjects *effective* control over their own data? This paper undertakes an interdisciplinary review of the concept of "control" to explore such questions in the fields of law and computer science.

DOI: 10.2966/scrip.120115.3

[*] Postdoctoral Research Fellow, Inria, Université de Lyon and Research Center Law, Informatics and Society (CRIDS), University of Namur.

[*] Research Director, Inria, Université de Lyon.

1. Introduction

As personal data processing technologies change and create new possibilities for tracking and tracing individuals, politicians and lawyers struggle to deal with the implications that these have for informational privacy and data protection. Many claim that these problems can be tackled with improved statutory drafting techniques and call for legislation that would give individuals greater *control* over the processing of their data. More than ever this notion of control dominates the contemporary conceptual and normative landscape of data protection and privacy.

Until now control has often been advocated as the key solution to the problems raised by personal data processing technologies.[1] Indeed, control is considered as a precious means of empowering the "digital self": It is deemed to foster autonomy through the ability to manage information about oneself and correspondingly offers some limited control over the way in which the individual is viewed by society. For this reason the notion of control is often mentioned, either explicitly or implicitly, as a core element of data protection policies.[2] In the recent EU Proposal for a general data protection regulation in particular a set of legal instruments are suggested that aim to put the data subject in control of his data. These include, for example, the explicit consent requirement, the withdrawal of consent, the right to be forgotten, the right to data portability, and the right to object.[3]

Despite the omnipresence of the notion of control in the EU policy documents, scholarly literature, and in the press the very meaning of the notion of control as well as its normative implications remains surprisingly vague and under-studied. From a fundamental rights perspective control in the sense of a set of "micro-rights" should undoubtedly be a central element of any empowerment policy in the field of privacy and data protection. However, in the face of recent technological developments and emergence of new social practices which seem to undermine the very capacity, if not the will, of individuals to "self-manage" their informational privacy this apparently simple and familiar notion becomes very ambiguous. What does it really mean to be in control of one's data in the context of contemporary socio-technical environments and practices? What are the characteristics, purpose and potential limits of such control and

---

[1] S R Peppet, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future" (2011) 105 *Northwestern University Law Review* 1153-1204, at 1183: "But even a cursory review of the literature should suffice to demonstrate that control dominates as the primary solution of privacy advocates".

[2] See our analysis of the EU policy documents below.

[3] See Article 4 (6) which provides a new definition of "data subject's consent"; Article 7 which clarifies the conditions for consent to be valid as a legal ground for lawful processing and introduces the right to withdrawal; Article 17 which provides the data subject's right to be forgotten and to erasure; Article 18 which introduces the data subject's right to data portability; Articles 19 and 20 which provide the data subject's rights to object and not to be subject to a measure based on profiling.

how can we guarantee individuals effective control over their own data? Is legislation on data protection an appropriate instrument for ensuring individual control?

In the field of privacy and data protection the challenge of grasping the notion of control is reinforced by the fact that two totally different meanings are frequently ascribed to this notion.[4] The first is structural/objective and relates to the risks associated with what G. Deleuze used to call "control societies".[5] In this respect, control refers to the notion of surveillance which can be exercised by public institutions or private companies in order to monitor, regulate and influence people's behaviour. The theme of *control as surveillance* has been extensively covered in the literature over the last decades and has recently regained prominence following the National Security Agency (NSA) scandal and, more importantly, the emergence of a new form of "algorithmic governmentality".[6] The second way to consider the notion of control is in an individual/subjective manner and relates to the multiple ways in which individuals interact with each other and communicate personal information: The ways in which they participate in the self-construction of their digital identities. In this sense c*ontrol as agency* refers to self-determination over information about oneself and self-management of privacy.

This second way of considering control will be the central focus of this paper. If one is to acknowledge that disclosure of personal data is part of the contemporary everyday life and practices of individuals, we contend that it is important to fully understand the meaning of control as well as to understand its pragmatic modalities. Hence, it is necessary to take the current rhetoric of control and empowerment seriously as advocated both in EU policy documents and by the proponents of the "privacy as control" theory.

This paper therefore undertakes an interdisciplinary review of the concept of "control" in the fields of law and computer science. Part 2 explores the meanings of the concept of control as it is developed in privacy and data protection scholarship. Beyond the currently fashionable rhetoric of empowering the data subject this part aims to identify and critically assess the characteristics of control and its normative consequences. Part 3 focuses on the operational dimension of control as deployed in several EU policy documents and legislation. This explores whether the institutional understanding of control at the EU level differs from that of academic scholarly literature and whether it goes beyond individual control to encompass organisational and technical measures as well. Part 4 examines the concept of control from a technical point of view; something which does not correlate exactly with the legal understanding. It reviews and analyses

---

[4] O Fuchs, "Towards an alternative concept of privacy" (2011) 9 *Journal of Information, Communication and Ethics in Society* 220-237, at 222.

[5] G Deleuze, *Pourparlers 1971-1990* (Paris : Les Editions de Minuit, 2003), at ch 5. See also K D Haggerty and R V Ericson, "The surveillant assemblage" (2000) 5 *British Journal of Sociology* 605-622.

[6] A Rouvroy and T Berns, "Gouvernementalité algorithmique et perspectives d'émancipation: le disparate comme condition d'individuation par la relation?" (2013) 31 *Réseaux* 163-196; J Cheney-Lippold, "A New Algorithmic Identity. Soft Biopolitics and the Modulation of Control" (2011) 28 *Theory, Culture & Society* 164-181.

the potential of various technical tools to make control more efficient. Finally, the concluding part attempts to reorient data protection scholarship towards a more comprehensive and refined understanding of the concept of control. In particular, it pursues the claim that taking control seriously requires focusing more strenuously on two fundamental and intertwined issues: control of *what* and control by *whom*?

2. The concept of control in data protection and privacy scholarship

The concept of control is of paramount importance to the literature on privacy and data protection. This concept is not new and, long before the Internet era, control over personal information had been considered as one of the dominant definitions of "privacy".[7] The "privacy as control" theory was constructed in reaction to the definition of privacy as the "right to be let alone" that was advocated by the famous attorneys Brandeis and Warren at the end of the nineteen century.[8] Conceived in this fashion privacy is a condition of insulation deemed to guarantee freedom from interference and intrusion upon the personal sphere. For many scholars, however, this conceptualization of privacy abusively conflates privacy with liberty and misleadingly suggests the existence of a private sphere (or "bubble") that surrounds the self and into which other individuals and organizations cannot encroach.[9] In contrast, the proponents of the control theory argue that privacy has nothing to do with protecting one's space from intrusion but is determined by the ability to control personal information.[10]

In the latter regard the most influential formulation of privacy is perhaps the one proposed by A. Westin (1967), who describes privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[11] The idea that privacy is the ability of the individual to control the terms under which personal information is acquired and used has been endorsed by a broad community of scholars. C. Fried (1968), for example, recognizes that being able to maintain control over personal information is crucial as it allows us to create the necessary context for relationships of respect, friendship and trust. For this author, "privacy is not simply an absence of

---

[7] H T Tavani and J H Moor, "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies" (2000) *Computer & Society* 6-11, at 6.

[8] L Brandeis and S Warren, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193-220.

[9] C J Bennett, "In Defense of Privacy: The Concept and the Regime" (2011) 8 *Surveillance & Society* 485-496, at 488.

[10] H T Tavani, "Privacy and the Internet" (2000) *Boston College Intellectual Property & Technology* available at http://www.bc.edu/bc_org/avp/law/st_org/iptf/commentary/content/2000041901.html (accessed 8 May 15). As H. Tavani points out the conception of privacy has evolve from one concerned with intrusion and interference to one that has been concerned with information:

> …it must be noted that recent theories of privacy have tended to center on issues related to personal information and to the access and flow of that information, rather than on psychological concerns related to intrusion into one's personal space and interference with one's personal affairs.

[11] A F Westin, *Privacy and freedom* (New York: Atheneum Press, 1967).

information about us in the minds of others; rather it is the control we have over information about ourselves."[12]

Along the same lines, J. Rachels (1975) argues that there is a close connection between the ability to control who has access to one's information and the ability to maintain a variety of social relationships with different types of people.[13] W. Parent (1983) also tried to provide a more detailed account of the control theory that does not overlap with other familiar values such as liberty, autonomy, solitude, secrecy, etc. He defines privacy in narrow terms as the condition of not having undocumented personal information known by others; therefore recognizing the importance of choice and control about "…facts that most persons in a given society choose not to reveal about themselves or facts about which a particular person is extremely sensitive and which he therefore does not choose to reveal about himself."[14]

Nowadays the "privacy as control" theory is more vivid than ever and has been also endorsed by more recent commentators dealing with the contemporary issues raised by complex digital environments, practices and devices. Current literature focuses more on informational privacy and data protection issues than on privacy *stricto sensu*[15] and the concept of control is more than ever advocated as the key solution to the problems raised by current personal data processing technologies.[16] Control is not only mentioned as a core element of conceptual reflections but also as a prescriptive remedy proposed by scholars.[17]

Current "privacy as control" theories emphasize the role of choice and individual self-determination over other values. In this regard, they can be described as information management theories where control is achieved through the subjective management and

---

[12] C Fried, "Privacy" (1968) 77 *Yale Law Journal* 475-493, at 482.

[13] J Rachels, "Why privacy is important" (1975) 4 *Philosophy & Public Affairs* 323-333, at 326.

[14] W A Parent, "Recent Work on the Concept of Privacy" (1983) 20 *American Philosophical Quarterly* 341-355, at 341. For Parent, personal information is "undocumented" in the sense that this information does not belong to the public record.

[15] It should be noted that the notion of control is currently mobilized in the field of privacy as well as in the field of data protection. We would like to stress here that privacy and data protection are not synonymous terms and that privacy must overall be considered as a broader notion. See J Kokott and C. Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" (2013) 3 *International Data Privacy Law* 222-228. Nevertheless, in the scholarly literature the notion of control is theoretically conceived in a more or less similar fashion in both fields.

[16] S R Peppet, see note 1 above, at 1183.

[17] P M Schwartz, "Internet Privacy and the State" (2000) 32 *Connecticut Law Review* 815-857, at 820 ("The leading paradigm…conceives of privacy as a personal right to control the use of one's data"); J E Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 *Stanford Law Review* 1373-1438, at 1379 ("Data privacy advocates seek…to guarantee individuals control over their personal data."); M R Calo, "The Boundaries of Privacy Harm" (2011) 86 *Indiana Law Journal* 1131-1162, at 1134 (describing privacy harms as "the loss of control over information about oneself or one's attributes"); J Litman, "Information Privacy/Information Property" (2000) 52 *Stanford Law Review* 1283-1314, at 1286 ("[A]ctual control [of information] seems unattainable.").

expression of personal preferences.[18] Accordingly, individuals are deemed to be able to determine what is good for themselves and consequently to decide to withhold or disclose more or less personal information.[19] Control is then conceptualized as an individual, dynamic and flexible process whereby people can either make themselves accessible to others or close themselves. As M. Birnhack puts it, privacy as control is "…the view that a right to privacy is the control an autonomous human being should have over his or her personal information, regarding its collection, processing and further uses, including onward transfers."[20] In this view, control takes the shape of the right of individuals to know what information about themselves is collected; to determine what information is made available to third parties; and to access and potentially correct their personal data.

Beside self-determination and self-management, informational privacy scholars have also conceptualized control and data subject's rights in terms of property. Indeed, an important part of the privacy literature has focused on property-based metaphors to sustain the argument that a greater control over personal information could be achieved through market-oriented mechanisms based on individual ownership of personal data. According to this view: "privacy can be cast as a property right. People should own information about themselves and, as owners of property, should be entitled to control what it is done with it."[21] Or as V. Bergelson puts it: "in order to protect privacy, individuals must secure control over their personal information by becoming real owners."[22]

In this view control over one's personal data is directly connected to the idea of legal or beneficial ownership.[23] In this sense the concept of control evokes the kind of absolute power or sovereignty over things that is conventionally associated with the property regime. Such a basic conception of property entails an "exclusivity axiom" which theoretically allows the owner to protect one's good from unwanted uses as well as granting him fully alienable rights.[24] In this conception, free alienability is considered as a quintessential aspect of any propertisation of personal data, and

---

[18] D J Solove, "Privacy Self-Management and the Consent Paradox" (2013) 126 *Harvard Law Review* 1880-1903.

[19] O Fuchs, see note 4 above, at 223.

[20] M D Birnhack, "A Quest for A Theory of Privacy: Context and Control. A Review of Helen Nissenbaum's Privacy in Context: Technology, Policy, and the Integrity of Social Life" (2011) 51 *Jurimetrics* 447-479, at 449. The author draws this definition from Allan Westin's 1967 seminal article.

[21] J Litman, see note 17 above, at 1287.

[22] V Bergelson, "It's Personal but Is It Mine? Toward Property Rights in Personal Information" (2003) 37 *University of California, Davis Law Review* 379-451, at 383.

[23] J B Baron, "Property as Control: The Case of Information" (2012) 18 *Michigan Telecommunications & Technology Law Review* 367-418, at 409 ("My argument has been that medical and other information is in at least one important way alike: it is information over which individuals seek control. It is control, I have argued, that has led to calls for the propertization of information.").

[24] C M Rose, "Canons of Property Talk, or, Blackstone's Anxiety" (1998) 108 *Yale Law Journal* 601-632, at 603.

controlling one's data would legally mean being entitled to trade and exchange it on the "privacy market".[25]

Despite being anchored in completely different legal backgrounds, both of these conceptions (control as self-determination and control as property) share common theoretical assumptions about privacy that originated in liberal worldviews. Indeed, the concept of control is strongly associated with the conventional figure of the "rational and autonomous agent", capable of deliberating about personal goals, controlling the course of the events and acting under the direction of such deliberation.

The sense of control that the liberal picture relies on is, first, *individualist*, in the sense that it emphasizes individual choice, self-governance and, overall, self-direction of one's life. In that regard the concept of control seems to confer to the data subject an extraordinary kind of sovereignty. It permits each individual to define, unilaterally and independently, their relationships with others. Moreover, in this view, privacy is conceived of as the separation of the self from others and society at large. Secondly, it is *active* in the sense that it stresses agency and construction of a life for oneself.[26] In this view, control over personal data cannot be reduced to the mere exercise of one's right to be let alone. Instead it refers to individual's ability or willingness to make decisions that control the use and sharing of information through active choice. Therefore this active choice implies, on the one hand, the effective participation of data subjects in the management of their data[27] and on the other, the liberty to alienate their data as long as this choice (and the subsequent alienation) is informed and voluntary.

At this stage of our analysis it should be noted that both the *individualist* and *active* dimensions of control have been subject to criticisms, which are sometimes even formulated by the proponents of control theory themselves who have developed more nuanced conceptual accounts. Space does not permit to engage in an in-depth discussion of the philosophical foundations of control theories however it is important to highlight, even succinctly, some of the main objections formulated.[28]

On one hand various authors question the very possibility of control by deconstructing the conventional figure of the "rational and autonomous agent" that is at the core of

---

[25] It should be noted that such a conception is much more in vogue among US scholars than among their European peers, who stay strongly attached to a human rights perspective and resist the idea that personal data could be assimilated as a mere commodity. However, there are a few notable exceptions. See, for instance, the claims of A. Bensoussan in: "Commission Nationale de l'Informatique et des Libertés, Vie privée à l'horizon 2020. Paroles d'experts" (2012) 1 *Cahier Innovation et Prospective* 46-53.

[26] R G Frey, "Privacy, Control and Talk of Rights" (2000) 17 *Social Philosophy and Policy* 45-67.

[27] A general assumption of control theory is that data subjects can be expected to behave as if they are performing a calculus (cost-benefit analysis) when assessing the outcomes that they will receive as a result of information disclosure.

[28] For a more in-depth discussion on this topic, see the works of the different authors mentioned below.

"privacy as control" theories.[29] Combining theories ranging from behavioural economics to sciences and technologies studies, from social psychology to human-computer interaction, they explore the multiple factors which play a role in our decision to protect or to share personal information with an emphasis on the cognitive and behavioural biases that hamper users' privacy decision making. As A. Acquisti and J. Grossklags point out in their works, at least three different factors might influence data subjects and alter their capacity to engage in privacy self-management: incomplete information, bounded rationality, and systematic psychological deviations from rationality.[30]

The first decisive factor relates to privacy literacy and, in particular, to the issue of incomplete information about privacy risks and insufficient knowledge about technological or legal forms of privacy protection.[31] Because of information asymmetries, data subjects are often unaware (or at least less conscious than data controllers and other entities) about the nature, extent and use of collected data. In the absence of sufficient information, privacy decision-making becomes undermined not only because of information asymmetries but also because of the lack of knowledge about the uncertainties and risks involved. Indeed, in the majority of cases data subjects may not be aware of the potential personal consequences of sharing and exchanging personal information. Incomplete information about the risks complicates privacy decision-making as it is very difficult for data subjects to adequately weigh the costs and benefits of revealing information, permitting its use or allowing its transfer without a refined understanding of the potential downstream consequences.[32]

Secondly, even if armed with complete information people might not be able to adequately process the vast amounts of data to reach a rational decision. As numerous studies have highlighted in the field of psychology and cognitive sciences, human rationality is bounded[33] and this "limits our ability to acquire, memorize, and process all relevant information, and it makes us rely on simplified mental models, approximate

---

[29] J Hanson and D Yosifon, "The Situational Character: A Critical Realist Perspective on the Human Animal" (2004) 93 *Georgetown Law Journal* 1-179; J Hanson and D Yosifon, "The Situation: An Introduction to the Situational Character, Critical Realism, Power Economics, and Deep Capture" (2003) 152 *University of Pennsylvania Law Review* 129-346.

[30] A Acquisti and J Grossklags, "What Can Behavioral Economics Teach Us About Privacy" in A Acquisti et al (eds), *Digital Privacy. Theory, Technologies, and Practices* (New York: Auerbach Publications, 2007) 363-377.

[31] S Trepte et al, "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)" in S Gutwirth, R Leenes and P de Hert (eds), *Reforming European Data Protection Law* (Dordrecht: Springer, 2014) 333-365.

[32] The issue of incomplete information and, more generally, of privacy literacy is at the core of the debate regarding privacy policies and other types of notices which aim to provide relevant information to data subjects and to help them make better decisions. Various studies have highlighted the problems raised by privacy policies in terms of information overload and cognitive costs. See R Calo, "Against Notice Skepticism in Privacy (and Elsewhere)" (2012) 87 *Notre Dame Law Review* 1027-1072.

[33] H A Simon, *Models of Bounded Rationality* (MIT Press, 1982); A Newell, *Unified Theories of Cognition* (Cambridge MA: Harvard University Press, 1990).

strategies, and heuristics".[34] Such bounded rationality can result in inconsistent behaviours and impede the ability of data subjects to formulate privacy-sensitive decisions. For instance, it affects the capacity of individuals to identify the various factors that might impact on their privacy. Most importantly, individuals experience real troubles comparing and calculating any gains and losses associated with the various strategies that they may choose in privacy-sensitive situations. Because humans are unable to appropriately "compute" all the information available they tend to reduce the cognitive costs associated with privacy self-management and, consequently, do not necessarily take steps to become informed about privacy risks.[35]

Other studies have also emphasized the influence of contextual variables on privacy decision-making. Individuals' privacy preferences are highly determined by the context and the way in which choices are framed[36], as in the case of opt-in/opt-out settings for example.[37] Along the same lines, individuals are seemingly more inclined to share personal information when the context makes them feel in control, regardless of the true or illusory nature of such control. While sharing their data with the members of social networks or with various providers, people might suffer from an "illusion of control".[38]

Third, even assuming the hypothetical case of access to complete information and full cognitive capacity to process it, actual control over personal data can still be affected by systematic psychological deviations from rationality. Various systematic behavioural anomalies and biases can have a serious impact on individual decision-making such as: immediate gratification, hyperbolic discounting, under insurance, and self-control problems amongst others.[39] In the privacy arena, an important bias that has

---

[34] A Acquisti and J Grossklags, "Privacy and Rationality in Individual Decision Making" (2005) *IEEE Security & Privacy* 26-33, at 27. See also K J Strandburg, "Privacy, Rationality and Temptation: A Theory of Willpower Norms" (2005) *Rutgers Law Review* 1235-1306.

[35] A M McDonald and L F Cranor, "The Cost of Reading Privacy Policies" (2008) 4 *I/S: A Journal of Law and Policy for the Information Society* 540-565, at 546. See also T Vila, R Greenstadt and D Molnar, "Why We Can't be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market" in L J Camp and S Lewis (eds) *The Economics of Information Security* (Kluwer, 2004) 143-154; G R Milne and M J Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices" (2006) 18 *Journal of Interactive Marketing* 15-29.

[36] R H Thaler, C R Sunstein, and J P Balz, "Choice Architecture" (2010) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583509 (accessed 8 May 15).

[37] N Lundblad et B Masiello, "Opt-in Dystopia" (2010) 7 *Script-ed* 155-165.

[38] L Brandimarte et al, "Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis" (2009) available at https://www.ideals.illinois.edu/handle/2142/15344 (accessed 8 May 15). These scholars formulate the hypothesis that individuals might suffer from an "illusion of control" when dealing with the publication of their data: "Namely, we hypothesize that when subjects are personally responsible for the publication of private information online, they may also tend to perceive some form of control over the access of that information by others, thereby confounding publication with access."

[39] A Acquisti and J Grossklags, see note 34 above.

come under scrutiny is the immediate gratification bias.[40] Individuals turn over their data for very small benefits or rewards;[41] they experience great difficulties in assessing the trade-offs between certain, immediate gains and speculative, long-term benefits.[42]

Besides the focus on the limits of data subjects' capacities of cognition and action, other attempts in the literature aim to overcome strictly individualistic accounts of privacy by paying attention to its collective aspects: privacy conceived as a common good or a social value. According to a growing number of scholars,[43] treating control over personal data solely as a matter of individual negotiation and party autonomy in contracting arrangements neglects the more socially oriented values underlying privacy. Taking control seriously implies understanding the collective and multi-relational dimensions that exist beyond the subjective preferences and individual strategies of both data subjects and controllers.

In place of liberalism's emphasis on the individual, these scholars stress the need to identify and evaluate the societal repercussions of data processing operations even in the cases were such operations have been initially legitimized by free and informed consent. As J. Cohen points out, these scholars "…have tried to move the concept of privacy well beyond control and individual consent, re-conceptualizing it in various ways as a social good that deserves protection for reasons beyond individual welfare".[44] By conceiving privacy as a common good or a social value, these authors share a common type of anthropology which might be depicted as "communitarian". Indeed, their arguments revolve around a strong emphasis on data subjects' membership and involvement in social groups and the community at large.

In this respect, these scholars bring the silent presence of a "third actor" back into the light. The processing of so-called "personal" data does not imply a mere bilateral scheme between the "concerned person" and the "data controller", but can simultaneously affect other actors, with either closer or more distant proximity to the "concerned" person. The notion of the "third actor" needs to be understood more or less strictly. In some instances the transfer of "personal" data can have serious consequences on close family members, especially in the case of medical data such as genetic

---

[40] A Acquisti, "Privacy in electronic commerce and the economics of immediate gratification" in *Proceedings of the ACM Conference on Electronic Commerce* (EC' 04) (2004) 21-29.

[41] See A Acquisti and J Grossklags, "Privacy and Rationality: A Survey" in K J Strandburg and D Raicu (eds) *Privacy and Technologies of Identity. A Cross-Disciplinary Conversation* (Springer, 2006) 15-30, at 16; N Good et al, "User choices and regret: Understanding users' decision process about consensually acquired spyware" (2006), 2 *I/S: A Journal of Law and Policy for the Information Society* 283-344, at 293.

[42] M Rabin and T O'Donoghue, "The economics of immediate gratification" (2000) 13 *Journal of Behavioral Decision Making* 233-250.

[43] See the works of the authors mentioned below.

[44] J E Cohen, "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen" (2001) 89 *Georgetown Law Journal* 2029-2049, at 2039.

profiles.[45] Similarly, the recent controversy surrounding the facial recognition system developed by Facebook illustrates the potential impact on members of a social network.[46] In its broadest sense the third actor represents the community as a whole and, consequently, the concept of privacy is re-conceptualized in terms of "social good" or "'foundational' human good", as A. Allen puts it.[47]

Along this line of thought, various authors contend that privacy and data protection are not only a matter of personal autonomy but also a social and democratic concern. For P. Schwartz information privacy should be conceived of as "constitutive value" and should not be considered as a right of control.[48] Indeed, "access to personal information and limits on it help form the society in which we live in and shape our individual identities".[49] By protecting and shaping private spheres that ensure the necessary independence for self-determination and self-construction, privacy enriches democracy. N. Richards has developed a theory of "intellectual privacy" in this regard, claiming that privacy is not only crucial to ensure self-development but also to furthering the richness of democratic debate.[50] Indeed, "…the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others" ensures people's intellectual development, which in turn shapes the "marketplace of ideas" and influences the originality and quality of public debate: a fundamental cornerstone of democratic society.[51] J. Cohen also contends that privacy "…is an indispensable structural feature of liberal democratic political systems".[52]

From a normative standpoint these non-individualistic accounts of privacy bring two intertwined issues to the fore, which radically question the relevance of the "privacy as control" theories. On the one hand some authors stress the urgent need to re-evaluate their consent-centric approach in light of the many problems associated with consent. As D. Solove point outs:

> The privacy self-management model attempts to be neutral about substance – whether certain forms of collecting, using, or disclosing of personal data are good or bad – and instead focuses on whether people consent to the collection, use, or disclosure of their data.

---

[45] L A Bygrave, "The Body as Data? Biobank Regulation via the 'Back Door' of Data Protection Law" (2010) 2 *Law, Innovation and Technology* 1-25.

[46] Y Welinder, "A Face Tells More Than Thousands Posts: Developing Face Recognition Privacy in Social Networks" (2012) 26 *Harvard Journal of Law & Technology* 165-239.

[47] A L Allen, *Unpopular Privacy: What We Must Hide* (Oxford University Press, 2011), at 13.

[48] P M Schwartz, see note 17 above.

[49] *Ibid*, 834.

[50] N M Richards, "Intellectual Privacy" (2008) 87 *Texas Law Review* 387-445.

[51] *Ibid*, 389.

[52] J Cohen, *Configuring the Networked Self* (Yale University Press, 2012), at 148.

> Consent legitimizes nearly any form of collection, use, and disclosure of personal data.[53]

On the other hand, given the societal dimension of privacy, other authors attempt to develop more substantive conceptions of privacy. They raise the issue of potential restrictions on personal autonomy which could lead, in some cases, if not to an abandonment of the logic of consent at least to the imposition of strict conditions on its implementation. For instance, some scholars have tackled the complex issues raised by alienability and in their works control ceases to be conceived of as an absolute and exclusive power but rather as a prerogative which in some instances can, or may even need to be, limited.[54] In some cases law should regulate certain types of data processing operations that would be otherwise destructive to democratic communities.

Despite these various attempts to refine the control theory in the field of privacy and data protection law and ethics, some commentators consider that the concept of control still remains too vague and ambiguous.[55] Although we do not disagree that control is a crucial issue, we share this argument.

We believe that, when defined purely in managerial terms, the concept of control can hardly be disentangled from other privacy theories. Indeed, the concept of privacy encompasses a myriad of definitions which all require to a certain extent some level of control from the user. In the literature, the systematic inclusion of elements of control in definitions of privacy is particularly obvious in the various attempts of classification proposed by different authors. For instance, in the taxonomy developed by D. Solove a number of different types of privacy are enumerated. Alongside "control over personal information" five other types of definitions are mentioned: (1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) personhood; and (5) intimacy.[56]

It is truly not clear what specifically distinguishes control over personal information from other types of actions or interests regarding privacy. To be sure, to be able to limit access, ensure one's right to be let alone and to secure confidentiality individuals must be able to exercise some degree of control over their personal information. If this is narrowly conceived in managerial terms the concept of control then seems to be an essential characteristic of any definition of privacy and loses a great deal of its potential

---

[53] D J Solove, see note 18 above, at 1880.

[54] P M Schwartz, "Property, Privacy and Personal Data" (2004) 117 *Harvard Law Review* 2055-2128.

[55] D W Shoemaker, "Self-exposure and exposure of the self-informational privacy and the presentation of identity" (2010) 12 *Ethics and Information Technology* 3-15, at 4. As Shoemaker points out, defining control simply as a matter of information management does not say anything about the extent of the control required nor about what specifically counts as the relevant zone of personal information that should be kept under control. See also H T Tavani, "KDD, data mining, and the challenge for normative privacy" (1999) 1 *Ethics and Information Technology*, 265-273.

[56] D J Solove, *Understanding Privacy* (Cambridge MA: Harvard University Press, 2008). See also D J Solove, "A Taxonomy of Privacy" (2006) 154 *University of Pennsylvania Law Review* 477-560 and the typologies proposed by H T Tavani, "Informational Privacy: Concepts, Theories and Controversies" in K E Himma and H T Tavani (eds) *The Handbook of Information and Computer Ethics* (Hoboken: Wiley, 2008) 131-164; K Gormley, "One hundred years of privacy" (1992) *Wisconsin Law Review* 1335-1441.

significance. Even among restricted access theories, which are conventionally opposed in the literature to control theories,[57] references to the notion of control seem inescapable. In these theories, one element of control concerns avoiding unwanted intrusion or interference by others into one's private space and, consequently, implies the limitation of other's access to the self[58] along with the control of personal boundaries[59] and environment.[60]

Overall we think that the ambiguity surrounding the concept of control is mainly due to a misleading conflation between the *conceptualization* and *management* of privacy. In order to reach a refined understanding of the notion of control and its link to privacy theories and polices it is therefore necessary to draw a distinction between the different uses and roles of this notion.[61] Accordingly, it is important to differentiate the conceptual dimension of control (i.e. control as conceptual foundation of privacy) from its instrumental dimension (i.e. control as a tool for the management of privacy). In the next section we will focus on the instrumental dimension of control as it has been deployed by EU institutions.

3. The notion of control in the EU policy documents

Over the last decades, the idea that individuals should have an effective control over their own data has become a key part of the rhetoric deployed by EU institutions in the field of data protection. In many policy documents,[62] control is advocated as an important tool for protecting privacy and achieving the empowerment of data subjects. In this section we will explore some of these documents to try and identify the main characteristics of the notion of control as it is featured in EU documents.

Before starting the analysis of these characteristics it is worth formulating a few preliminary remarks. Firstly, the notion of control is mentioned in documents of very diverse nature, ranging from: preparatory works for legislation and legislative text, to experts' opinions, to vulgarized material addressed to citizens etc. This diversity illustrates the pervasiveness of the rhetoric of control in the field of data protection. Second, as we will see hereafter, in most of these documents the notion of control takes the shape of a toolbox at the disposal of the data subjects: they are equipped with a set of subjective "micro-rights" which supposedly enable them to be in control at the

---

[57] H T Tavani, see note 56 above, at 142.

[58] R Gavison, "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal*, 421-472.

[59] I Altman, "Privacy: A Conceptual Analysis" (1976) 8 *Environment and Behavior* 7-29. For Altman, privacy is conceived of as a "boundary control process"; the selective control over access to oneself.

[60] C Goodwin, "Privacy: Recognition of a Consumer Right" (1991) 10 *Journal of Public Policy & Marketing* 149-166. For Goodwin, privacy includes two dimensions of control: control over the presence of others in the consumer's environment and control over information dissemination.

[61] Along the same lines see H T Tavani and J H Moor, "Privacy Protection, Control of Information, and Privacy-Enhancing technologies" (2001) *Computers & Society* 6-11. For these authors, any relevant theory of privacy should distinguish between three components: concept, justification and management.

[62] See notes 63 to 68 below.

different stages of the processing of their data. Thirdly, the notion of control appears to have a much more extended meaning than in the scholarly literature given the operational/instrumental dimension of EU policy documents.

Here is a limited list of EU documents mentioning the notion of control in the recent years:

- 2013 Proposal for a general data protection regulation;[63]
- 2012 Communication from the Commission, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21th Century;[64]
- 2012 European Commission brochure and movie "Take control of your personal data";[65]
- 2011 Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent;[66]
- 2010 Communication from the Commission, A comprehensive approach on personal data protection in the European Union;[67]
- 2009 Article 29 Data Protection Working Party, "The Future of Privacy.[68]

---

[63] See the draft of the *General Data Protection Regulation*, Unofficial consolidated version after LIBE Committee vote provided by the Rapporteur, available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf (accessed 8 May 15).

[64] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committees of the Regions, *Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21th Century*, COM(2012) 9 final, Brussels, 25 Jan 2012, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en (accessed 8 May 15).

[65] European Commission (DG Justice), *Take control of your personal data* (Luxembourg: Publications Office of the European Union, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf (accessed 8 May 15).

[66] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, available at

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (accessed 8 May 15). See II.3 "related concepts"; control is explicitly mentioned among other important concepts relating to consent (alongside with informational self-determination, autonomy and transparency).

[67] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committees of the Regions, *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 4 Nov 2010, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (accessed 8 May 15).

[68] Article 29 Data Protection Working Party, *The Future of Privacy*, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 01 Dec 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (accessed 8 May 15). See the reference made to the "empowerment of the data subject", at 15.

For the sake of clarity we will focus on two documents which, despite their distinctive nature, are highly representative of the current rhetoric of control fostered by EU institutions.

The first document is the communication adopted by the European Commission in 2012 titled *Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*. This communication is part of the works pertaining to the reform of the EU's data protection framework. From the very beginning of this document it is explicitly stated that, "[i]n this new digital environment, individuals have the right to enjoy *effective control* over their personal information."[69] Following this logic the first half of the communication is entirely dedicated to the theme of control, as featured in particular in section two: "Putting individuals in control of their personal data".

This document mentions a number of different issues raised by digital environments which undermine the effectiveness of data protection rules: the lack of harmonization of the member states legislations and the data protection national authorities; the ever-increasing volume of collected data; the perception of loss of control by citizens amongst others.[70] Relying on this overview of the situation, the communication then recalls one of the main ambitions of the new legislative act proposed by the Commission: "The aim…is to strengthen rights, to give people efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively."[71] In order to achieve this aim, the Commission proposes a set of new rules which will: "improve individuals' ability to control their data"; "improve the means for individuals to exercise their rights"; "reinforce data security"; and "enhance the accountability of those processing data".[72]

More precisely, four objectives are mentioned which are supposed to empower the data subjects to "improve individuals' ability to control their data".[73] Foremost among these objectives is the principle of consent and the reinforcement of the related legal requirements. This comes as no surprise as consent remains a cornerstone of the EU approach to data protection. Indeed, from a fundamental rights perspective it is conventionally considered as the "best way for individuals to control data processing

[69] See note 64 above, at 2 (emphasis added).

[70] *Ibid*, 4.

[71] *Ibid*, 5.

[72] *Ibid*, 6-7.

[73] *Ibid*, 6.

activities."[74] Although consent plays a key role in giving control to data subjects,[75] it is not the only way to do this. The Commission also aims at equipping individuals with a right to be forgotten, guaranteeing data accessibility portability and reinforcing the right to information.[76]

In addition to this "bundle" of rights, the communication equally points to other rules that are deemed to foster more effective management of personal information. Very interestingly the Commission seeks to reinforce control through additional rules which are of a radically different nature than the micro-rights granted to the data subject. They consist of an heterogeneous set of organizational and technological tools such as: (i) improved *administrative and judicial remedies* via a strengthening of national data protection authorities' independence and powers along with enhancing administrative and judicial remedies when rights are violated; (ii) reinforced *security measures* through encouragement of the use of privacy-enhancing technologies, privacy-friendly default settings and privacy certification schemes; and (iii) increased *responsibility and accountability*, in particular by requiring data controllers to designate a data protection officer in combination with the introduction of a "privacy by design" principle and obligation to carry out data protection impact assessments for organizations involved in risky processing.[77]

At the other end of the spectrum, it is also worth paying attention to a second document issued by the European Commission in 2012. This document explicitly titled *Take control of your personal data* is a small brochure published to raise awareness among EU citizens about the new legal reform and, more precisely, about the changes that will strengthen citizens' rights in the field of data protection.[78] With the help of simplistic slogans, garish fluorescent fonts and fancy drawings the Commission tries to convey its message to the general public:

> Every time you go online you share information about yourself. And the more you do online the more important it is that you and your personal data are protected. The EU is proposing changes that will strengthen your protection online. The new EU laws are designed to

---

[74] Committee on Civil Liberties, Justice and Home Affairs (Rapporteur J. Ph. Albrecht), *Report on the General Data Protection Regulation)*, 21 Nov 2013, at 200, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN (accessed 8 May 15). See also Opinion 15/2011 of the Article 29 Data Protection Working Party, note 66 above, at 8.

[75] C Lazaro and D Le Métayer, "Le consentement au traitement des données à caractère personnel : une perspective comparative sur l'autonomie du sujet" (2015) 48 *Revue Juridique Themis* 765-815.

[76] See note 64 above, at 5-6.

[77] *Ibid*, 6-7.

[78] See note 65 above. The publication of this brochure was accompanied by the release of a short film available at http://ec.europa.eu/justice/data-protection/minisite/users.html (accessed 8 May 2015).

> *put you in control of your own information* and safeguard your right to personal data protection."[79]

Despite its naïve comic strip-like format, it is interesting to observe that the approach to control deployed in this document is structured along the same lines as the aforementioned communication. Indeed, alongside the micro rights granted to data subjects,[80] the brochure also refers to other organizational or technological instruments which are supposed to foster control such as: contact points (where to go and who to talk to in case of problems); privacy by default (making the settings of all websites privacy-friendly and allowing the changing of privacy settings by users); notification of breaches to the concerned person(s) and the Data protection authority where data has been lost or stolen; and, more globally, the harmonization of protection across the EU.

The overview of these two radically different documents published by EU institutions in the recent years reveals a much more entangled approach to control than appears in the scholarly literature. In these documents the framing of privacy and the implementation of data protection through control has a dual nature, both individual/subjective and organizational/structural.

On one side, the granting of a set of micro-rights to the data subject echoes the main tenets of the control theories: the empowerment of the subject through individual choice and participative agency.[81] In that sense the concept of control refers to the individual's ability to make a decision about personal data through autonomous choice. According to the rights-based approach embedded in EU policy documents and legislation, the rational and autonomous data subject is equipped with tools which will improve the way he or she can control the conditions under which their personal information is collected, used, and transferred. Eventually, this "legal equipment" aims at transforming the data subject in an active agent who can (and ought to) shape their own digital lives.[82]

On the other side, although the individual remains the main agent of control and of the decision-making process in the rhetoric developed by the EU institutions, the notion of control is extended beyond strictly individualistic approaches. In particular, the regulator mobilizes a more operational notion of control that cannot be reduced to the

---

[79] The same "slogan" is repeated at the very end of the brochure: "The new EU laws will *put you in control* of the information about yourself that you share online. They'll give you the right to know who's using your data and why and to know if the security of your data is at risk..." (emphasis added).

[80] The brochure especially mentions the right to a better information in order to help people in the decision-making process (whether to share their personal information); the consent requirements (explicit permission and withdrawal of consent); the right to be forgotten (to delete permanently the data after one has shared them); and the right to data portability (to remove the data and give it to another service provider).

[81] O Fuchs, see note 4 above, at 220. In that sense, as Fuchs points out, "[c]ontrol theories are subjective theories…because they stress the dependence of privacy on human subjectivity and individual action and choosing."

[82] However, note that the regulator imposes in some circumstances substantial limits to the liberty to alienate data (see the case of "sensitive data").

purely subjective and mental activity of an autonomous data subject. For the regulator, it is also clear that individual control cannot be exercised without putting a "control architecture" in place, namely a set of structural measures that aim at creating a reliable and secure environment for the data subject. Framed in such a way control over personal data is not treated solely as a matter of individual negotiation and party autonomy in contracting arrangements, but rather as an operation that is also potentially dependent on other important "environmental" variables: technological (i.e. security measures, privacy by default settings, etc.) and organizational (i.e. the accountability of data controllers, privacy impact assessments, etc.).

On closer examination, the analysis of the EU documents shows the diversity of normative tools that data subject have to be equipped with in order to attain control over their own data and, more globally, to keep up with technological change.[83]

4. Control from a technical point of view

The previous sections have shown that the notion of control is multifaceted, but most of the interpretations of control, if not all, assume that the subjects must be able to act, in one way or another, to exercise their rights. In the digital world these actions are mostly carried out through information technologies. A relevant question at this stage is therefore: what does control mean in the technical world, and can technologies provide appropriate tools to support the notions of control proposed by lawyers and philosophers?

Firstly, it is worth noting that the view of control as a set of "micro-rights" in the fundamental rights perspective is very much in line with the view of control in computer science.[84] One of the most common uses of the term "control" in this area can be found in the expression "access control" in computer security. Access control refers to techniques for restricting access to a resource (for example personal data) to authorised users. Interestingly, a difference is made in computer security between discretionary access control, in which the owner of an object defines the rules, and mandatory access control, in which the rules are defined by the system administrator. This difference raises the question: who is the actor in charge of defining the rules of access? In other words, who is "in control"?

Another interesting observation about the notion of control in computer security is that its use has been extended to "usage control", precisely for the purpose of providing

---

[83] Such a diversity of tools is also characteristic of the "mixed approach" developed in the new Proposal for a general data protection regulation. Although the data subject's control is one of the strategic objectives targeted by the Proposal there is no explicit reference to the concept of control among the legal provisions. However, it is mentioned in recital 6 which states that "*individuals should have control of their own personal data*" while insisting on the need to build a strong and more coherent data protection framework in the Union in order to foster the digital economy and reinforce certainty for all the actors (emphasis added). See also recital 51a.

[84] The word "control" has been used in different areas of computer science, but the focus here is on the uses of the word having a connection with privacy or exhibiting features which can be transposed to privacy.

ways to implement legal provisions in the area of intellectual property.[85] In contrast with access control, usage control makes it possible to control the object during its usage, for example to enforce time limitations or a maximum number of uses.[86] Usage rights can also be conditioned to certain obligations.[87] Usage control can typically be useful for implementing Digital Right Management, but there have also been suggestions that it could be applied to personal data management to limit the uses, for example, to the declared purpose or to express the need to obtain the consent of the subject.[88]

In the context of operating systems control also includes other "micro-rights" such as the rights to create, read, modify or delete a file and the right to get access to a directory list. These rights can be granted to individuals or to groups of users.[89]

To sum up, the different variants of control in computer science can be classified according to two main criteria: the *subject* of the control (who is in charge of the control?) and the *object* of the control (what does the subject control?).

As far as privacy enhancing technologies are concerned one must admit that they mostly reflect the individualistic view discussed in section two. However, as we will show, the collective dimension of control is also supported by some recent tools. With respect to the object of the control three main categories of tools can be identified. The first one, sometimes called "transparency enhancing technologies" (TETs), basically supports the right to be informed: the right of the subject to know what happens to his or her personal data. The second supports all "active rights" of the subject such as the right to express consent or to have data modified or deleted. The third one supports "negative rights" such as the right to prevent the disclosure of data (or, in other words, to ensure the implementation of the "data minimization" principle).

In the remainder of this section we first study the object of control (and the aforementioned three types of rights) in subsection 4.1 before discussing the subject of control (and the individual versus collective views) in subsection 4.2 and concluding with some reflections on the relativity of control in subsection 4.3.

4.1 The object of control: a set of micro-rights

The exercise of control rights requires a deliberate action on the part of the subject, meaning that not only should the system make this action possible but also that it should provide sufficient information to allow the subject to ensure that he can properly

---

[85] J Park and R Sandhu, "The UCONABC usage control model" (2004) 7 *ACM Transactions on Information and System Security* 128-174, at 131-133.

[86] *Ibid*, 137.

[87] *Ibid.* 133-139.

[88] *Ibid.* 166-169.

[89] See for example https://en.wikipedia.org/wiki/File_system_permissions (accessed 8 May 15).

understand the situation and take well-informed decisions. The first type of technologies that provides valuable support to the subject in this phase are sometimes referred to as the "transparency enhancing technologies" (TETs).[90]

4.1.1 Transparency enhancing technologies (TETs): the right to be informed

TETs can take different forms depending on the context and the type of information provided to the user. As far as web sites are concerned the simplest forms of TET are the "privacy icons" which are visual signs designed to make it possible to see at a glance the main features of the privacy policy of the site (data collected, purpose, deletion delay, etc.). Users can then parameterize their privacy policy in such a way that their browser can automatically check whether the policy declared by a site meets the user's requirements and to inform them (for example through specific icons) of the result of the verification.[91]

Some websites also provide a dashboard functionality informing users of the personal data stored[92] and identifying third parties who can acquire access to it. However this kind of site must have very carefully designed interfaces to ensure that they do not mislead users.[93] For example, the European PrimeLife project has proposed a Firefox extension called Privacy Dashboard that would allow users to know some of the practices of the websites they are using; for example whether they use cookies, geolocation, third party content or other tracking means. An icon displays a happier or sadder face depending on the overall evaluation of the web site.[94]

Specific solutions have also been proposed to improve the privacy interfaces of social networks. Such solutions aim, for example, to reduce unnoticed over-sharing of information, to make it easier to find out to whom a particular attribute is visible,[95] or to help users avoid making posts that they may later regret.[96]

---

[90] M Hildebrandt and B-J Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era" (2010) 73 *The Modern Law Review* 428-460.

[91] Privacy Bird is an example of browser add-on (for Internet Explorer) that provides this opportunity.

[92] Google Dashboard provides this opportunity but shows only a subset of the collected data.

[93] For example, Scott Lederer et al identify five pitfalls for designers (obscuring potential information flow, obscuring actual information flow, emphasizing configuration over action, lacking coarse-grained control and inhibiting existing practice) and show existing systems either falling into these pitfalls or avoiding them: S. Lederer et al, "Personal privacy through understanding and action: Five pitfalls for designers" (2004) 8 *Personal Ubiquitous Computing* 440-454.

[94] PrimeLife, "Bringing sustainable privacy and identity management to future networks and services" (2008-2011) available at http://primelife.ercim.eu (accessed 8 May 15).

[95] T Paul, D Puscher and T Strufe, "Improving the Usability of Privacy Settings in Facebook" (2011) *CoRR* abs/1109.6046.

[96] Y Wang et al, "I regretted the minute I pressed share: A Qualitative Study of Regrets on Facebook" in *Proceedings of the Seventh Symposium on Usable Privacy and Security* (New York: ACM, 2011) 10:1-10:16.

Personal data is sometimes collected without the subject being aware of it and by parties that the subject has never heard about. This happens typically through cookies created on a computer while browsing and which are subsequently used by a variety of companies to track the subject's activities and, ultimately, to generate personalized advertisements based on the subject's browsing profile. Users can get a picture of the covert tracking going on by using a tool like Lightbeam[97] (formerly Collusion) which is a Firefox add-on recording the events associated with visited sites. This tool allows users to display a graph showing tracking sites and their interactions. Several tools such as TaintDroid[98] or Mobilitics[99] have also been proposed for smartphones which represent another major source of personal data leaks.

4.1.2 Active Rights: consent, modification, deletion, etc.

When a decision has been reached about privacy preferences the next step for a data subject is to express this decision. Several techniques are available to help in this task which differ mostly in terms of scope (general purpose versus specific) and interfaces. On the general purpose side a number of languages have been proposed for the expression of privacy policies.[100] The general principle is that both the subject and the controller (typically a web site) should be able to author privacy policies which are translated into a machine readable format. The policies can then be processed automatically and matched to ensure that a controller collects only personal data associated with a privacy policy (defined by the subject) in a manner consistent with their own policy. As an illustration, tools like P3P[101] and Privacy Bird[102] allow respectively websites to declare their privacy policies and visiting users to have these policies analysed and compared with their own preferences. Depending on the result of the matching, different icons can be displayed in order to inform the user to make a decision whether to accept and visit the site, refuse, or to look further into their own privacy policy (in which case Privacy Bird can also be used to display the policy in a

---

[97] Lightbeam for Firefox available at http://www.mozilla.org/en-US/lightbeam (accessed 8 May 15).

[98] W. Enck et al, "TaintDroid: An Information-flow Tracking System for Realtime Privacy Monitoring on Smartphones" in *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation* (Vancouver: Usenix, 2010) 1-6.

[99] J P Achara et al, "Mobilitics: analyzing privacy leaks in smart phones" (2013) 93 *ERCIM News* available at http://ercim-news.ercim.eu/en93/special/mobilitics-analyzing-privacy-leaks-in-smartphones (accessed 8 May 15).

[100] See for example A Barth et al, "Privacy and Contextual Integrity: Framework and Applications" in *Proceedings of the 2006 IEEE Symposium on Security and Privacy* (IEEE Computer Society, 2006) 184-198; M Y Becker, A Malkis and L Bussard. "S4P: A Generic Language for Specifying Privacy Preferences and Policies" (2010), Technical report MSR-TR-2010-32, Microsoft Research; D Le Métayer, "A Formal Privacy Management Framework" in P Degano, J Guttman and F Martinelli (eds) *Formal Aspects in Security and Trust. 5th International Workshop FAST 2008 Malaga, Spain, October 9-10, 2008 Revised Selected Papers* (Springer Verlag, 2009) 162-176; A Barth et al, "Privacy and utility in business processes" (2007) *Proc. CSF*, 279-294.

[101] Platform for privacy preferences (P3P). See "W3C Technical report" (2002) available at www.w3.org (accessed 8 May 15).

[102] Privacy Bird available at http://www.privacybird.org (accessed 8 May 15).

user-friendly way, starting with a summary). The user preferences can be set through a number of panels allowing a choice of different levels of protection for different types of data (health, financial, etc.).

However this approach raises several challenges. For this kind of consent to be legitimate from a legal point of view it must be *free*, *specific*, *informed* and *unambiguous*.[103] For example, the categories of data that can be used in P3P or Privacy Bird may be too coarse in many situations and as a result may force the users to disclose more data or grant to third parties broader rights than they would really like to. Most languages may also lead to ambiguities or statements that can be interpreted in different ways. Ambiguities may arise for example from the use of vague terms and from the complexity of interpreting combinations of rules.[104] One of the criticisms raised against early privacy frameworks such as P3P was their lack of clarity and their divergent (or even misleading) representations of privacy policies.[105]

An option to solve the ambiguity problem would be to resort to a sound, mathematical definition of the semantics of the language. This approach has been followed in several proposals such as CI[106] and S4P[107] and SIMPL.[108] However, even though their scope goes beyond the definition of privacy policies[109] and they offer the potential of a strong future impact these academic results have not moved out into the field. One reason why these languages have not been deployed is the fact that their generality creates new needs in terms of the user interface: to be truly usable they should be integrated within tools allowing users to express their choices in a convenient and efficient way. Indeed, the users of such tools are not assumed to be knowledgeable in mathematics and should be able to interact with the system through user-friendly interfaces, which have not been developed for these languages yet.

---

[103] *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, available http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN (accessed 8 May 15).

[104] C A Brodie, C-M Karat and J Karat, "An empirical study of natural language parsing of privacy policy rules using the Sparcle policy workbench" in *Proceedings of the Second Symposium On Usable Privacy and Security* (New York: ACM, 2006) 8-19.

[105] J Reidenberg and L F Cranor, "Can User Agents Accurately Represent Privacy Policies?" (2002) available at http://ssrn.com/abstract=328860 (accessed 8 May 15).

[106] A Barth et al, see note 100 above.

[107] M Y Becker et al, see note 100 above.

[108] D Le Métayer and S Monteleone. "Computer assisted consent for personal data processing" in *Proceedings of the 3d LSPI Conference on Legal Security and Privacy Issues in IT* (LSPI'2009) 29-41.

[109] They can be used to specify norms in a more general sense. For example CI has been applied to HIPPA (Health Insurance Portability and Accountability Act), COPPA (Children's Online Privacy Protection Act) and GLBA (Gramm-Leach-Bliley Act).

Another option provided by some browsers is the Do Not Track (DNT)[110] feature that allows users to express a choice not to be tracked in their browsing activities. This opt-out choice is communicated to visited websites through a specific DNT HTTP header sent every time data is requested from the Web.[111] However, there is no consensus yet on how web sites should precisely interpret this DNT signal. In addition, there are no legal requirements for its use and no way to enforce it from the user's side. As a result, many sites simply ignore it while others may limit the amount of information that they collect.[112]

More generally, the actual enforcement of privacy choices depends very much on the localization of the personal data. In fact the only decisions of the data subject that can be enforced locally are choices concerning cookies, popups or ad blockers. These choices are implemented on the device of the subject and so, as long as they know how to do it, subjects can also decide at any time to erase cookies stored on their computer[113] or their browsing history. The enforcement of all other types of consent relies on the existence of appropriate technical means on the side of the controller (and, in some cases, of other stakeholders) and their proper execution. The subject has therefore no choice but to put some trust on the data collector: they must trust them to have such technical means in place and to not try to bypass them. As discussed in the next subsection, this trust could be enhanced through compliance audits conducted by independent third parties.

As suggested above, one technical option to ensure the implementation of privacy policies is to resort to DRM like technologies to monitor the use of personal data.[114] Personal data would then be managed in the same way as digital content (e.g. video or music). Unfortunately it is not clear whether this solution is really viable considering that personal data would easily be copied after it is output from the DRM system to be used for the purpose. Experience has also shown that DRM techniques can often be bypassed with moderate effort: as stated by M. Hilty, D. Basin and A. Pretschner, "[a]t the very least, DRM can act as a support mechanism…and thereby increase the

---

[110] Do Not Track is provided by the Firefox browser for example: See Mozilla Foundation "Do Not Track" (2015) available at https://www.mozilla.org/en-US/firefox/dnt/ (accessed 8 May 15).

[111] W3C Tracking Protection Working Group, Tracking Preference Expression (DNT), http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html (accessed 8 May 15).

[112] See C Hoffman, "Why Enabling 'Do Not Track' Doesn't Stop You From Being Tracked" (2012) available at http://www.howtogeek.com/126705/why-enabling-do-not-track-doesnt-stop-you-from-being-tracked/; Athena Privacy, "Do Not Track Statement Survey" (2014) available at http://www.athenaprivacy.com/images/Athena_Do_Not_Track_Survey_Alexa_100_20140302.pdf (accesses 8 May 15).

[113] This may not always be obvious for non-technical users though. For example, they may not be aware of the fact that different types of cookies may be stored on their computer, some directly by their browser and others by Adobe Flash Player, each of which requires different actions.

[114] V Mayer-Schönberger, "Beyond Copyright: Managing Information Rights with DRM" (2006) 84 *Denver University Law Review* 181-198.

likelihood that the obligations are fulfilled, or at least prevent unintended violations resulting from carelessness."[115]

Another extreme solution would be to require data controllers to use a trusted computing environment to process personal data. Such a trusted platform ensures that the system behaves as expected at the price of having a unique encryption key loaded in the hardware and made inaccessible to the user. This solution has been used in specific cases such as healthcare information processing,[116] but it remains to be seen whether it can become a more widely adopted solution considering the controversies surrounding the trusted computing technology itself, which entails the removal of some control of the users over their own computers[117] (and correspondingly increases the control of the computer manufacturers and software providers).

4.1.2 Negative rights: non-disclosure, data minimisation

Other technologies (sometimes called "privacy enhancing technologies" or PETs) are also available to enforce privacy rights.[118] The main goal of PETs is to reduce as much as is possible (or even to prevent) the disclosure of personal data, typically through the use of cryptographic techniques. For example, it is possible to use PETs to implement a smart metering system in which the operator does not get any personal data regarding the users apart from their quarterly fee. This is made possible through a combination of architectural choices (the fee is computed locally, on the equipment of the users) and appropriate cryptographic protocols (to ensure that the users are accountable and that they cannot cheat on the computation of the fee).

This notion of "privacy by architecture" differs from the usual vision of "privacy by control" as the user does not have to take any action: the design of the system ensures that his or her personal data will not be disclosed. To use the Latourian terminology, one can say in that case that control is entirely delegated to non-human actors.

---

[115] M Hilty, D Basin and A Pretschner, "On obligations", in *Proceedings of the 10th European Symposium on Research in Computer Security* (Berlin: Springer, 2005) 98-117, at 107.

[116] CBI Health, "Data Protection for Regulatory Compliance" (2008) available at http://www.trustedcomputinggroup.org/files/resource_files/3B1360F8-1D09-3519-AD75FFC52338902D/03-%20000216.1.03_CBIHealth.pdf (accessed 8 May 15).

[117] Which is, admittedly, the intended effect for privacy enforcement when the trusted execution environment is on the side of the data controller since the objective is to force him to fulfill the sticky privacy policies.

[118] I Goldberg, "Privacy-Enhancing Technologies for the Internet III: Ten Years Later" in A Acquisti et al (eds), *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications, 2007) 3-18; G Danezis and S Gürses, "A critical review of 10 years of privacy technology in *Proceedings of Surveillance Cultures: A Global Surveillance Society?*" (UK, 2010) available at http://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf (accessed 8 May 15); C Diaz and S Gürses, "Understanding the landscape of privacy technologies" (2012) https://www.cosic.esat.kuleuven.be/publications/article-2215.pdf (accessed 8 May 15); Y Shen and S Pearson, "Privacy Enhancing Technologies: A Review" (Laboratories HP, 2011) available at http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf (accessed 8 May 15).

This analysis is also in line with the distinction made by some authors between hard privacy and soft privacy[119] which are associated with different trust assumptions. Hard privacy (as illustrated by PETs) tries to avoid, as far as is possible, placing any trust in a third party (or to reduce this trust), while soft privacy is based on the assumption that the subject will, technically speaking, lose control over their data and therefore will have no choice but to place a certain amount of trust in the data controller. In the latter situation technologies for enforcing the rights of the subject can be seen as ways to reduce this "loss of control" and to organize it in the best interest of the subject.

4.2 The subject of control: individual versus collective views

The above discussion about "privacy by architecture" versus "privacy by control" also echoes the debate on the "individualistic" versus "collective" views of control and privacy: "privacy by architecture" can be seen as a form of collective control because the decision to implement privacy protections is imposed by an authority which is supposed to represent the interests of the subjects as a whole. Ideally, the design of the system could even be approved or certified by an independent third party.

This collective view of privacy, even if not dominant in the technological landscape, is supported by other types of tools. For example, irrespective of the actual level of information that they can obtain, one could argue that individuals are always in a weak position when they have to take decisions about the disclosure of their personal data because they generally do not have the necessary expertise to fully understand all the legal and technical aspects of the situation.

One solution to redress this imbalance is to provide some form of collaboration between individuals to help them analyse privacy policies and warn each other about unacceptable terms. Terms of Service; Didn't Read (ToS;DR)[120] is an example of effort in this direction. The goal of ToS;DR is to create a database of analyses of the fairness of privacy policies and to make this information available in the form of explicit icons (a general evaluation plus any good and bad points) which can be expanded if needed into more detailed explanations. Users can also install a browser add-on to get the ratings directly when they visit a page. A key aspect of ToS;DR is the fact that users can submit their own analysis for consideration, the goal being that, just like Wikipedia, a group consensus will emerge to provide a reliable assessment of each policy. This type of tool is especially interesting as they promote a broader notion of control which is less individualistic and more collective, even if the final decision always pertains to the subject.

Accountability (at least in its strongest forms, when it requires auditability by independent third parties) can also be seen as a form of collective approach in the sense

---

[119] M Deng et al, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements" (2011) 16 *Requirements Engineering* 3-32.

[120] ToS:DR available at http://tosdr.org (accessed 8 May 15).

that it ensures that the subject is not left alone in front of the data controller. The key idea behind the notion of accountability is that data controllers should not merely comply with data protection rules but should also be able to demonstrate compliance or "showing how responsibility is exercised and making this verifiable", as stated by the Article 29 Working Group.[121] Technologies can facilitate accountability through the privacy policy languages and frameworks mentioned above. They can also contribute to accountability of practices to ensure that data controllers can be in a position to demonstrate that their practices, and hence their use of personal data, complies with their obligations.

The main piece of evidence for accountability of practices should be the execution logs of the system. However, for accountability to really keep its promises these logs have to meet a number of requirements:[122] they must contain sufficient information to establish compliance (or detect non-compliance) and they must reflect the actual behaviour of the system (bypassing the log architecture to hide certain operations or to provide false evidence should be difficult). Moreover, their security must be guaranteed. In particular, it should not be possible to modify them and non-authorized users should not be allowed to read their content. Technologies are already available to support log secure storage[123] and to analyse them to conduct audits.[124] These should be complemented with precise procedures to ensure that audits are conducted by independent third parties, which could be a data protection authority or a private auditor with a valid accreditation from a data protection authority. Legal sanctions should also be imposed in case of non-compliance (or failure to implement appropriate accountability measures).[125]

In practice, data protection authorities should keep the power to supervise on a regular basis the activities of the auditors themselves, in order to ensure that they maintain a high evaluation standard. As pointed out by the Article 29 Working Party, "putting the accountability principle into effect will provide useful information to data protection authorities to monitor compliance levels. Indeed, because data controllers will have to be able to demonstrate to the authorities whether and how they have implemented the

---

[121] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (accessed 8 May 15), at 7 (§ 21).

[122] D Butin and D Le Métayer, "A guide to end-to-end accountability" in *Proceedings of the TELERISE Conference* (IEEE, 2015).

[123] M Bellare and B S Yee, "Forward integrity for secure audit logs", Technical report (San Diego: University of California, 1977); B Schneier and J Kelsey, "Secure Audit Logs to Support Computer Forensics" (1999) available at https://www.schneier.com/paper-auditlogs.pdf (accessed 8 May 15)

[124] See, for example: D Garg, L Jia, A Datta, "Policy Auditing over Incomplete Logs: Theory, Implementation and Applications" in *Proceedings of 18th ACM Conference on Computer and Communications Security* (New York: ACM, 2011) 151-162; D Butin and D Le Métayer, "Log Analysis for Data Protection Accountability", *19th International Symposium on Formal Methods (FM 2014)* (Springer Verlag, 2014) 163-178.

[125] D Butin, M Chicote, and D Le Métayer, "Strong Accountability: Beyond Vague Promises" in S Gutwirth, R Leenes, and P de Hert (eds), *Reloading Data Protection* (Dordrecht: Springer, 2014) 343-369.

measures, very relevant compliance related information would be available to authorities. They will then be able to use this information in the context of their enforcement actions."[126] Another major benefit of accountability is that it can act as an incentive for data controllers to take privacy commitments more seriously and put appropriate measures in place, especially if audits are conducted in a truly independent way and followed by sanctions in case of breach. As pointed out by P. de Hert, "this qualitative dimension of accountability schemes should not be underrated".[127]

4.3 Control as a relative notion

Paradoxically, the term "control" as interpreted by lawyers seems to be used as a key privacy principle in situations where "control", in the technical sense, is effectively relinquished (or at least shared) by the subject. Indeed, in most situations subjects actually lose the control over their personal data as soon as they disclose it in so far as they cannot have a 100% guarantee concerning the use of their data by the data controller. This should not imply that control is a meaningless or illusory principle, but this observation nonetheless argues in favour of an interpretation of control as a relative notion. The main lesson to be drawn from this analysis is therefore that technical means are available to enhance control but lawyers and policy makers should avoid overreliance on the notion of control because it cannot be, from a practical point of view, an absolute protection.

5. Conclusion

More than ever the notion of control plays a pivotal and pervasive role in the discourse of privacy and data protection. Privacy scholarship and regulators propose to increase individual control over personal information as the ultimate prescriptive solution: it is considered a crucial means of managing digital identity and empowering the data subject. Nevertheless, at a time of ever-increasing digitalization and global circulation of data such rhetoric seems at odds with the current reality of control we are able to exercise over our digitalized lives. Indeed the premise of autonomy and active agency implied in this rhetoric seems to be radically undermined in the context of contemporary digital environments and practices. Exploring this ambiguity from an interdisciplinary perspective, this paper reviews the different meanings of the notion of control and tries to clarify the characteristics of this notion as developed in several sources of literature and EU policy documents.

As we have seen, the policy or regulatory initiatives in the field of data protection described in this paper represent a more entangled approach to control than the strict individualistic paradigm of the "privacy as control" theory developed in the scholarly

---

[126] See note 121 above, at 16 (§ 60).

[127] P de Hert, "Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law" in D Guagnin et al (eds) *Managing Privacy Through Accountability* (Basingstoke: Palgrave Macmillan, 2012) 193-232, at 200.

literature. In the EU policy documents control is conceived as a dual notion, both individual and structural. In the eyes of the regulator the burden of controlling personal information cannot only weigh on the data subject's shoulders. For control and the related "micro-rights" granted to the data subject to be effective they must be supported by structural measures.

The (ab)use of the fashionable rhetoric of control by policymakers tends then to obscure this structural dimension, but even a cursory review of the EU policy documents reveals that the idea of control is not dissociated from the implementation of organizational and technical measures. This shows that the regulator is aware that control over personal information cannot only be a matter of individual agency. Control cannot be properly achieved if the data subject is not put in a position to monitor whether the data controller actually complied with their privacy preferences. Similarly, control becomes almost impossible when the data subject has to deal with privacy-unfriendly default settings and technologies. Therefore the regulator seeks to reinforce individual control by additional rules which consist of a heterogeneous set of organizational and technological tools to foster such control; for instance, measures to ensure accountability and privacy by design mechanisms.

Despite their appeal to an extended and operational meaning of the notion of control, we argue that EU policymakers fall short of grasping the crucial issues raised by the notion of control. This is mainly due to the fact that they still remain excessively attached to the individualistic paradigm according to which the data subject is depicted on the basis of the conventional "rational and autonomous agent": a monadic and abstract individual capable of deliberating about personal goals and of acting under the direction of such deliberation.[128] The reliance on this overtly simplistic account of human agency impedes further investigation of the pragmatic modalities of the operation of control and, more specifically, inhibits apprehension of the normative consequences of two fundamental questions: control of *what* and control *by whom*? Taking control seriously requires thus raising the issues of the *object* and the *subject* of control.

The first question raised by the theme of control relates to the definition of its object. What is the target of individual control and can it be limited to personal information as it is defined in data protection legislation? What does it really mean to be in control of one's data in the context of contemporary socio-technical environments and practices? Nowadays individual control can certainly not be considered as a panacea to the thorny issues raised by "Big Data phenomenon" and ever-evolving data mining and profiling practices. In particular, individuals are often not aware or do not understand how this happens, who collects their data and how to exercise control. The use and further transfer of personal data is very often done in an extremely complex and non-transparent way. This situation of course strongly undermines the very idea of control.

---

[128] S R Peppet, see note 1 above, at 1188. Peppet brilliantly observes that, despite their effort at reconceptualization, privacy scholars did not abandon the idea "…that individuals do and should remain the locus of the decision-making about their personal data".

Besides the voracious collection and use of personal information the big data phenomenon also raises the issue of control over large amounts of data which cannot be included in the category of "personal data" as it is currently defined by the legislation. Indeed, the construction of profiles by private and public organizations is based as much (if not more) on "impersonal" data as it is on personal data provided (voluntarily or not) by the individuals.

For some scholars one of the main drawbacks of the current EU legal framework is its excessive and misleading focus on so-called personal data. This "fetishisation"[129] of personal data obscures the true risks associated with data mining and profiling activities: the issues of information asymmetries upsetting the current balance of power between different protagonists, the risks of wrongful discriminations of people on the basis of particular characteristics[130] and, more fundamentally, the emergence of new modes of governance which undermine the very existence of legal and political subjects.[131] Moreover, the conventional split between personal and anonymous data tends to fall apart as "re-identification" techniques become more sophisticated allowing computer scientists to "deanonymize" individuals hidden in anonymised data with disconcerting ease.[132] For C. Priens, "[t]his then will require a debate on the role of the public domain in providing the necessary instruments that will allow us to know and to control how our behaviour, interests and social and cultural identities are 'created'."[133]

The second fundamental question raised by the theme of control relates to the determination of its subject/agent and implies an interrogation of the skills and competences of contemporary data subjects. Who are these data subjects and are they really able to cope with the ever-growing complexity of digital environments? Who can be said to be "in control"?

As has been unveiled these last years by research in the field of behavioural economics, cognitive sciences and human-computer interaction, the complexity is such that our judgments in this area are prone to errors stemming from: lack of information or computational ability; problems of self-control; and biased decision-making processes. For instance, time and attention are limited; it is impossible to control every single piece of information about oneself which circulates on the networks through myriads of channels and databases. Another consequence of the emphasis on active

---

[129] A Rouvroy, "Des données sans personne: le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data" in *Le numérique et les droits et libertés fondamentaux. Etude annuelle du Conseil d'Etat* (Paris : La Documentation française, 2014) 407-421, at 418. For A. Rouvroy the current "fetishisation" of personal data, which is reinforced by the characteristics of the legal framework itself, contributes to obscure the real nature of the problems raised by the phenomenon of Big Data.

[130] B Schermer, "The limits of privacy in automated profiling and data mining" (2011) 27 *Computer Law & Security Review* 45-52.

[131] A Rouvroy, see note 129 above.

[132] P Ohm, "Broken Promises of Privacy: Responding to the Surprizing Failure of Anonymization" (2010) 57 *UCLA Law Review* 1701-1778.

[133] C Priens, "When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?" (2006) 3 *Script-ed* 270-303, at 272.

choosing/control is the difficulty raised by the situations where people prefer not to choose. Indeed, the costs imposed on data subjects can be so high in complex and technical areas they are unfamiliar with that the majority of them tend to "stick" to default options instead of exercising their freedom of choice and being in control of the situation.[134] How can one reconcile the idea of control with the cognitive and behavioural biases that hamper users' privacy and security decision making?

On a more analytical level, even in the hypothetical case, where the data subjects would be perfectly aware and competent, the logic of control assumes (perhaps too rapidly) that voluntary disclosure of personal information causes no privacy problems.[135] However, we believe that it is nearly impossible for data subjects to really measure the breadth of their disclosure and the long term effects of their actions. It is thus very unlikely that they do not suffer harm even from a potentially informed, autonomous and responsible decision.[136]

For these different reasons the issue of the agent of control should be addressed with much more caution and attention than is currently the case. Although proponents of control theory and policymakers rightly recognize the importance of control they put so much emphasis on its subjective dimension that they fail to adequately capture the limits of the normative and technical tools at the disposal of data subjects. If actual empowerment and meaningful autonomy of data subjects are to be achieved granting them "micro-rights"[137] and providing them with privacy management technologies is certainly not enough. Indeed, the complexity of digital environments and practices is such that one should not expect data subjects to become privacy experts[138] and bear all the risks and responsibilities of privacy management alone.

---

[134] The issue at stake here is: How can control theory reconcile active choosing/control with "the choice of not to choose"? See C Sunstein, "Choosing not to choose" (2014) 64 *Duke Law Journal* 1-52.

[135] Note that one of the logical limits of the control theory becomes obvious in the case of total disclosure. What if a data subject willingly decides to reveal every single piece of information about oneself? Can one still argue that he retains privacy? One can have control, but no privacy: "The prospect of someone revealing all of his or her personal information and still somehow retaining personal privacy, merely because he or she retains control over whether to reveal that information, is indeed counter to the way we ordinarily perceive of privacy." H T Tavani, see note 10 above, at 2.

[136] Although recent literature has tried to reinvestigate the concept of privacy, there is still much work to do when it comes to identifying and evaluating what constitutes a privacy harm and its link with the (loss of) control over personal data. D J Solove, see note 56 above; R Calo, see note 17 above.

[137] Such as the right to be informed; the right to revoke consent; the right to access, modify, rectify, and delete the data; the right to data portability; the right to be forgotten; the right to object, etc.

[138] D J Solove, see note 18 above, at 1901:

> With the food we eat and the cars we drive, we have much choice in the products we buy, and we trust that these products will fall within certain reasonable parameters of safety. We do not have to become experts on cars or milk, and people do not necessarily want to become experts on privacy either. Sometimes people want to manage their privacy in a particular situation, and they should be able to do so. But globally across all entities that gather data, people will likely find self- management to be a nearly impossible task.

For control to become more than an empty notion one should embrace the idea that people act and transact in society not simply as individuals in an undifferentiated social world, but as individuals with certain capacities, in distinctive socio-technical contexts. This necessarily implies an integration of our understanding of the data subject's agency with the inescapable collective dimension of control. To put it simply, control over information cannot become effective until it is conceived and implemented in terms of shared engagement and cooperation between different human and non-humans actors.[139]

On one hand, the various modes of cooperation with non-human actors and the delegation of actions to machines has to be tackled more carefully. In digital environments the exercise of control is highly mediated by technical devices which can enhance but also hinder an agent's capacity to make choices and determine the course of his or her action. In this regard privacy management technologies deemed to provide more transparency and to allow more granular control over privacy settings do not necessarily solve the users' problems because they can increase their cognitive costs without addressing the underlying cognitive and behavioural biases.[140] As we have seen in section 4, the diversity of technical tools at the disposal of data subjects as well as their intrinsic working often adds another layer of complexity.

On the other hand, treating control over personal data solely as a matter of individual negotiation and party autonomy in contracting arrangements neglects the underlying relations of power between actors as well as the collective impact of privacy management beyond individual welfare. In this regard, making control meaningful implies envisioning and creating new modes of relations and cooperation between human actors (data subjects, public institutions, and private organizations) which would enable a more balanced distribution of risks and responsibilities. In the current *Proposal for a general data protection regulation*, EU legislators have already taken a few steps in this direction by imposing new obligations on data controllers[141] and by taking into consideration situations where there is a significant imbalance between parties.[142]

---

[139] See B Nardi, "Studying context: A comparison of activity theory, situated action models and distributed cognition" (1992) available at http://www2.physics.umd.edu/~redish/788/readings/nardi-ch4.pdf (accessed 8 May 14): "...it is not possible to fully understand how people learn or work if the unit of study is the unaided individual with no access to other people or to artifacts for accomplishing the task at hand." See also B Latour, *Pandora's Hope: Essays on the Reality of Science Studies*, (Cambridge MA: Harvard University Press, 1999), at ch 6.

[140] Moreover, this raises the problem of "familiarity" with technical artifacts and the nature of human agency which is involved in data subjects' daily idiosyncratic engagements with machines. See L Thévenot, "Le régime de familiarité. Des choses en personne" (1994), 17 *Genèses* 72-101.

[141] See, for instance, the new provisions regarding responsibility and accountability (Article 22), privacy impact assessment (Article 33) and the notification of a personal data breach to the supervisory authority (Article 31).

[142] See Article 7, § 4 of the Proposal: "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller."

Alternatives to classical regulation – such as "nudge"[143] or "crowdsourcing"[144] – could also presumably offer new ways to make control more effective.

In offering a brief overview of the two fundamental questions raised by control our goal is to foster discussion and encourage a more nuanced understanding of the concept. For the empowerment of the data subject to be effective we believe that there is an urgent need to develop an account of agency of data subjects which takes into consideration the multi-dimensional and varied intersections between individual capabilities and socio-technical environments, including the engagement of the individuals in meaningful participation and collective activity. In the absence of such reconceptualization the idea of control over personal information pervading current legal and political debates about privacy will amount to nothing more than a fairy tale.

Acknowledgement. This work was partially funded by the European project PRIPARE/FP7-ICT-2013-1.5, the European project PARIS/ FP7-SEC-2012-1, and the Inria Project Lab CAPPRIS.

[143] R Calo, "Code, Nudge or Notice?" (2014) 99 *Iowa Law Review* 773-803.

[144] See note 120 above.