Four Theses on Digital Mass Surveillance and the Negotiation Of Privacy

Antonio A. Casilli

Four Theses On Digital Mass Surveillance And The Negotiation Of Privacy

Antonio A. Casilli

Telecom ParisTech (Paris Institute of Technology)
EHESS (School for Advanced Studies in Social Sciences)

1. The current[1] political debate is fueled by growing tensions over the implementation of a digital mass surveillance framework aimed to gather, store and process data from transactions, interactions and everyday uses of information and communication technologies. In the wake of Edward Snowden's early revelations about the US PRISM program and the subsequent international scandal over the NSA/Five Eyes spying, surprise and shock among the general public were mostly due to the extent to which the intelligence agencies of western democratic governments were intercepting information from their own citizens. The subsequent legislative moves in France[2], United Kingdom[3], Canada[4], and Australia[5], towards long-term mandatory data retention and real-time algorithmic electronic surveillance are still met with strong opposition and suspicion from the civil society. They have been hurried into laws only at the price of strenuous efforts by governments and legislators to silence opposition, by failing to engage in democratic debate in the name of national security and the fight against terrorism.

2. Historically, the deployment of digital mass surveillance systems has been consubstantial with a long-term shift towards the expression of a powerful executive, combined with the infiltration of military interests in the democratic apparatus, or

[1] This text is a slightly revised version of my concluding contribution to the 'Report On Digital Technology And Fundamental Rights' of the French Council of State. Casilli, Antonio A. (2014). Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée. In: J. Richard & L. Cytermann (eds). Etude annuelle 2014 du Conseil d'Etat "Le numérique et les droits fondamentaux". Paris: La Documentation Française: 423-434.

[2] Loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825; Projet de loi relatif au renseignement n. 2669, 2015 http://www.assemblee-nationale.fr/14/projets/pl2669.asp

[3] Data Retention and Investigatory Powers Act 2014 http://services.parliament.uk/bills/2014-15/dataretentionandinvestigatorypowers.html

[4] Anti-terrorism Act, 2015 https://openparliament.ca/bills/41-2/C-51/

[5] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375

even by the gradual assimilation between domestic security matters and the doctrine of national security.[6] Although the executive power's tendency to operate with no counterbalance could be seen as part and parcel of a democratic project that is still *in fieri* (an 'unfinished democracy', to borrow French political theorist Pierre Rosanvallon's[7] expression), the securitarian shift Western countries have endured in the last decades stands apart by the way it has grown into an all-encompassing discourse influencing the methods of democratic deliberation, obstructing the ability of the legislative and judicial branches to check and balance executive functions on the one hand, and the manifestations of a general willingness to respect citizens' freedoms and fundamental rights on the other.

3. The fact that these events are poised to force a profound change to the relationship between governments and those they govern is only one of the variables of the current political equation. The other variable contributing to an unprecedented climate of political instability is represented by the fact that markets are increasingly playing less of a role as third party forces correcting states' securitarian excesses. As stakeholders in the digital economy fail to comply with their own responsibilities in limiting authoritarian allocations of powers, their passive or active roles in the creation of a vast military-industrial complex become clearer. We enter a phase of anxiety and distrust between consumers and private sector businesses as well. In the space where the political challenges of digital technologies are played out, economic and strategic interests of tech companies promote such surveillance methods, maintaining they simply build on the tools that modern states have long used to monitor populations. Conversely, governments push for more privacy-invasive surveillance techniques, on the grounds that the commercial entities are already taking liberties with citizens' personal data[8]. Indeed, this public/private sector feedback loop represents a clean break with past approaches of centralized surveillance.

THESIS 1: SURVEILLANCE HAS BECOME PARTICIPATORY

4. The current debate over mass surveillance is trapped within a false dichotomy between privacy and security. This opposition is instrumental to the promotion of the indiscriminate collection of personal data, which is seen as the only guarantee against the domestic and external threats that democracies face. The main tool of this erosion

[6] Périès, Gabriel (2013). Les dilemmes européens de la gestion des identités numériques : entre la confiance et la sécurité nationale. CVPIP (Personal Data Values and Policies Chair), Paris, Institut Mines-Télécom, 17 September http://cvpip.wp.mines-telecom.fr/2013/09/17/deuxieme-rencontre-de-la-chaire-le-mardi-17-septembre-2013-de-17h-a-19h-a-linstitut-mines-telecom/

[7] Rosanvallon, Pierre (2000). La démocratie inachevée. Histoire de la souveraineté du peuple en France. Paris: Gallimard.

[8] Grubb, Ben (2014). Metadata ambiguity to be resolved by government data retention policy paper: sources. Sydney Morning Herald, August 22, http://www.smh.com.au/digital-life/digital-life-news/metadata-ambiguity-to-be-resolved-by-government-data-retention-policy-paper-sources-20140822-1078o9.html; Champeau, Guillaume (2015). L'Assemblée adopte les boîtes noires qui surveilleront votre comportement. Numérama, April 16, http://www.numerama.com/magazine/32809-l-assemblee-adopte-les-boites-noires-qui-surveilleront-votre-comportement.html

of citizens' rights to privacy and secrecy is the rhetorical expedient of *seeking a balance*, a fair ratio between the collective right to security and the individual right to confidentiality. However, as highlighted by privacy advocate Caspar Bowden at an inquiry held by the British parliament's Intelligence and Security Committee in 2014, 'balance is a misleading metaphor. It tends to connote an unstable equilibrium with a single balance point on a linear scale'.[9] Achieving an optimal balance relies on a representation of privacy and public security as sitting in a continuum—of privacy being *intrinsically insecure* since it suspends surveillance.

5. Yet, the privacy-security continuum has been disrupted by a change in the nature of surveillance itself. In comparison with past ones, the current digital surveillance system for the monitoring populations is unique in that *it is not direct, but rather participatory.*[10] By 'participatory', we mean a mutual, horizontal surveillance based on the intentional, agonistic disclosure of personal information by users of digital services, mobile applications and online platforms. It is accompanied by a loss of control over the terms of service of technical infrastructures where personal data are stored and circulated. This surveillance is participatory insofar as it is mutual and involves a generalization of bottom-up moderation mechanisms and of the way online communities enforce norms within social platforms. A symbolic transition thus takes place, from surveillance practices relying on a Big Brother vertical conception to those relying on a 'Big Other' horizontal one, embodying a move towards an overwhelming social injunction to real-time connectivity[11]. Without this presupposition, surveillance programs based on direct access to large data collections would have been inconceivable. The surveillance system is constantly fed by the very subjects it monitors, who are part of a social system that rewards participation based on reciprocal disclosure aimed to build online social capital. Connected citizens are not just passive subjects and participatory surveillance does not inhibit their will. Rather, it empowers users by making them responsible for implementing the measures needed for the surveillance, as well as sorting through the duration and quantity of data to be disclosed, depending on the context.

6. Insofar as the quantity of disclosed data is actually determined by criteria that govern day-to-day ICT-mediated sociabilities and not by the need to protect the citizens, the search for a balance or fair ratio between privacy and security proves illusory.

7. We should not see the fact that citizens contribute to these social platforms as a symptom of technological illiteracy or ideological adherence. On the contrary, it should be viewed as a sign that their streams of communication are presently captured

---

[9] Bowden, Caspar (2014) Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament. London, February 7, http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf

[10] Albrechtslund, Anders (2008) Online Social Networking as Participatory Surveillance. First Monday, 13 (3), http://firstmonday.org/ojs/index.php/fm/article/view/2142

[11] Zuboff, Shoshana (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, Journal of Information Technology, 30 (1): 75–89.

by a participatory architecture that uses traces of online presence to personalize usage and record data transfers in digital environments.[12] The order of priorities between protecting privacy and personalizing digital user experience therefore seems reversed in the face of these traces, whose durability and secondary uses (for both commercial and securitarian purposes) are lost on users.

THESIS 2: CLAIMS THAT 'THE END OF PRIVACY IS NIGH' ARE ERRONEOUS AND IDEOLOGICALLY MOTIVATED

8. The issue of privacy – which has inevitably and painfully been at the very center of political and social debates in recent years – reveals the limits of a theoretical stance that has dominated media discourse and the public opinion for some time. This stance focuses on the reports of the 'end of privacy' and sees its alleged disappearance from our everyday life and political concerns as a prelude to its abrogation from our legal systems.

9. The Hypothesis of the End-of-Privacy has in large part been advocated by corporate interests groups and in particular tech giants[13]. An imaginary line connects the 1999 press conference during which the Chairman and Managing Director of Sun Microsystems, Scott McNealy, declared 'You have zero privacy anyway. Get over it!'[14] and the 2013 Federal Trade Commission event where Vint Cerf, in his capacity as Google's 'Chief Internet Evangelist', claimed that from a historical point of view, 'privacy may be an anomaly'.[15] This perspective sits within a highly stylized, politically focused narrative of the transition to modernity. According to this view, our societies have moved from a social structure characterized by small local communities where each individual had a thorough knowledge of the opinions and whereabouts of friends and neighbors, to an urban society where the idea of a private sphere of action and thinking has been imposed by the emerging middle classes. Today, the historical parenthesis of privacy would supposedly be about to close, as part of an inevitable and spontaneous transformation of behaviors and beliefs of social media users. The 'new norm', according to the definition given by Mark Zuckerberg in 2010 [16], is one of transparency and publicness. This change is seen as part of a longer historical transition. It legitimizes connectivity services that are based on extracting consumers' personal data by incorporating them into a wider collective process. The web giants'

[12] Merzeau, Louise (2013) L'intelligence des traces. Intellectica, 59 (1): pp.115-135.

[13] Tubaro, Paola, Casilli, Antonio A. & Yasaman Sarabi (2014). Against the Hypothesis of the End-of-Privacy. An agent-based modelling approach to social media, New York: Springer.

[14] Sprenger, Polly (1999). Sun on Privacy: "Get Over It". Wired, January 26, http://archive.wired.com/politics/law/news/1999/01/17538

[15] Ferenstein, Gregory (2013). Google's Cerf Says "Privacy May Be An Anomaly". Historically, He's Right. TechCrunch, November 20, http://techcrunch.com/2013/11/20/googles-cerf-says-privacy-may-be-an-anomaly-historically-hes-right/

[16] The Zuckerberg Files (2010) Facebook CEO Mark Zuckerberg: TechCrunch Interview At The Crunchies, transcript, January 8, http://dc.uwm.edu/zuckerberg_files_transcripts/32/

spokespeople want nothing less than to show that their aim is to put an end to the isolated and alienated existence of the great industrial cities of the last few centuries.

10. In an attempt at historical and cultural restoration, the outcome of the fully networked society tech giants aim to, would be the return to a time that they portray as one of harmony and openness among primary circles of socialization.

11. Within academia and the civil society, some embrace the Hypothesis of the End-of-Privacy while stigmatizing the attitudes and behaviors of individual ICT users as paradoxical and alarming.[17] They maintain that members of online and mobile social platforms would be prepared to gradually give up their privacy in order to benefit from commercial advantages and that usages would be moving towards greater transparency, in a regime of generalized sharing where monitoring by governments goes hand in hand with private companies tracking. Although inspired by quite different theoretical and political motivations from commercial stakeholders, academics who support this approach end up in agreement with the digital economy pundits they are trying to disprove – that privacy has well and truly disappeared.

However, observed behaviors run counter to this conclusion. In this ideologically charged climate, users are making increasingly insistent demands for autonomy and personal and collective empowerment. They are not remaining passive in the face of widespread complicity between businesses and governments, scandals surrounding the passing of draconian laws and the lack of legal and technical means to protect the integrity and confidentiality of personal data. To claim that this is the case, as certain ill-informed commentators have done, is misleading.

12. The distrust among users and producers of technologies goes hand in hand with a growing demand for services that secure and anonymize online interactions.[18] The increasing popularity of encryption tools, of 'anonymous' networks such as Tor, of 'amnesic' operating systems such as Tails, of 'ephemeral' websites and applications are all clear indications of the growing interest for users' control over their online presence. Although commercially motivated, and to a degree ineffectual, these are to be considered as technological responses to a collective demand for privacy protection solutions. Outside commercial offer, the proliferation of fake social media profiles and of quick-and-dirty presence optimization tacticts over the last few years are clear cultural signs of how users anticipate surveillance and put in place ad-hoc procedures to circumvent it[19].

13. Internet giants have reacted to this climate of distrust by offering 'competitive privacy services' (such as Gmail making it easier to encrypt emails, or Facebook

---

[17] Norberg, Patricia A., Horne, Daniel R. &, David A. Horne (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs, 41 (1): 100-126.

[18] Rainie, Lee, Kiesler, Sara, Kang, Ruogu & Mary Madden (2013). Anonymity, Privacy, and Security Online. Pew Research Center's Internet & American Life Project, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

[19] Pailler, Fred & Antonio A. Casilli (2015). S'inscrire en faux : les fakes et les politiques de l'identité des publics connectés. Communication, 33(2) [forthcoming].

allowing anonymous login) or by paying outrageous prices to acquire businesses that allegedly minimize the collection of metadata (e.g. the 19 billion dollars Facebook paid for WhatsApp in 2014). On the flip side, other sectors of the digital economy are suffering the repercussions of this new cultural and political awareness, such as US cloud computing providers, who stand to lose up to an estimated 35 billion dollars over three years.[20]

14. Whether it is motivated by commercial interests or political concerns, the historical narrative that underlies the Hypothesis of the End-of-Privacy remains therefore controversial. Rather than a smooth, linear transition from a world where privacy plays a central role to one where it has supposedly lost its *raison d'être*, we are today engaged in a full-fledged culture war over confidentiality, anonymity, and secrecy.

15. There is no guarantee that this war will be won by civil liberties advocates or by governments, with the complicity of big data-fuelled companies that currently uphold the system of mass participatory surveillance. Today, more than ever, we need to break free of the ideological framework in which we have become trapped, one that paints privacy as just a fortuitous historical circumstance.

THESIS 3: RATHER THAN FADING AWAY, THE 'CARE OF PRIVACY' INCREASINGLY PERMEATES ICT-MEDIATED SOCIABILITIES

16. Contrary to the received wisdom that privacy is disappearing, the importance attributed to managing the limits and content of citizens' personal spheres is in fact growing in the current social and technological climate. After Michel Foucault's notion of 'care of the self'[21], the *care of privacy* can be described as the task of defining the boundary between public and private—in other words, between collective responsibilities and constraints, and that which pertains to the individual capacity to think and act.

17. To break free of the current ideological biases, we need to re-contextualize the historical origins of the notion of privacy. According to Philippe Ariès' reconstruction of this historical process, the initial point can be set in Middle Ages, characterized by a social life that was neither private nor public in the sense we use these terms today. Before the modern era, interactions in the public space still fashioned an indistinct sphere where individual intimacy was dispersed in a network of 'collective, feudal and community' structures 'within a system that just about functioned: the solidarities of

[20] Castro, Daniel (2013). How Much Will PRISM Cost the U.S. Cloud Computing Industry?. Washington, DC: The Information Technology & Innovation Foundation, http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry

[21] "The task of testing oneself, examining oneself, monitoring oneself in a series of clearly defined exercises, makes the question of truth – the truth concerning what one is, what one does, and what one is capable of doing – central to the formation of the ethical subject.", Foucault, Michel (1984) Le Souci de soi, Gallimard, Paris.

the seigniorial community, those of lineage and vassal relations'. [22] As the balances of power that supported these structures were gradually dismantled, allowing the distinctive features of the private sphere to emerge—not just an abstract possibility, but rather a concrete concern that affects and permeates into the activities and personal orientations of modern individuals. Over the centuries, this care has been actualized by social measures that reflect this shift in attitude, such as *analyzing oneself through writing*, aided by the widespread elimination of illiteracy and the invention of printing; autonomous and egalitarian relationships, with an emphasis on *friendship* between peers; and the *reconfiguration of living space*, with a preference for private accommodations over communal and family houses.

18. All of these transformations can be seen as echoing the 'changes in the "We-I" balance' referred to by Norbert Elias.[23] Significantly, the 'social turn' of the Internet of recent years has continued this trend through an increasing emphasis on writing about oneself online, forging elective friendships and reconfiguring human spatiality. In doing so, it has made the care of privacy, as well as the public demand to protect it, more widespread.

19. The appearance of the notion of the private sphere is situated between the end of the Middle Ages and the onset of the Modern Era. Yet, the idea of privacy as a right and a prerogative to be defended is much more recent. Philosopher John Deigh [24] links its emergence to the need to provide a solution to the problem of the 'tyranny of the majority', first set out by Alexis de Tocqueville. The formidable strength of public opinion and the authority of the majority in modern democracies can become a threat to the autonomy of individuals and minorities. The need to guarantee intellectual freedom and to decide on a set of rights that moderate the government's power over individuals led the philosopher John Stuart Mill to formulate his 'harm principle'. According to this principle, the private sphere is an inviolable area of freedom. Mill states that 'The only part of the conduct of anyone for which he is amenable to society is that which concerns others. In the part that merely concerns himself, his independence is, of right, absolute'. [25] The discussion over the protection of privacy is part of such political and philosophical debate. Continuing this liberal tradition, Samuel Warren and Louis Brandeis set out the now canonical definition of the 'right to privacy' in their 1890 article published in the *Harvard Law Review*.[26] By developing the harm principle to take into account the need to guarantee not only the freedom to act but also the very ability of individuals to conceal themselves and their 'domestic circles' from public scrutiny, they defined privacy as 'the right to be left alone'.

---

[22] Ariès, Philippe (1986). Pour une histoire de la vie privée. In Id., Duby, G., Chartier, R. (eds). Histoire de la vie privée, tome 3 : De la Renaissance aux Lumières. Paris: Seuil.

[23] Elias, Norbert (1991). La société des individus. Paris: Fayard.

[24] Deigh, John (2012) Privacidad, democracia e internet', Internet y el Futuro de la Democracia, Champeau, S. and Innerarity, D. (eds.), Paidós, Barcelona.

[25] Mill, John Stuart (1859). On Liberty. London: John W. Parker & Son: 22

[26] Warren, Samuel & Louis Brandeis (1890). The Right to Privacy. Harvard Law Review, 4 (5): 193-220.

20. As Deigh highlights, this legal innovation was inherent to the technological context and media environment of the late 19th century. In the period when Warren and Brandeis were writing, it was mainly gossip press, photojournalism and investigative journalism that urged to set out the limitations of one of the very postulates of contemporary democracies: a 'well-informed citizenry'.

21. More than a century after this first definition of the right to privacy, digital media have become instruments to exert citizenship rights. It has therefore become imperative to examine the ways in which they affect the technological ecosystem in order to reproblematize the boundary between private and public. To a large extent, digital social technologies can be regarded as extensions of the 19th and 20th century tools used to document and capture images and other multimedia contents as proof of behaviors and individual opinions. They also make concerns over managing and restricting their effects more widespread. By looking at the issue from a historical perspective, we can see how the supposed 'new social norm' of publicness advocated by corporate interests, but feared by users, hides a completely different reality. Privacy protection remains a key concern, but it undergoes a qualitative transformation that leads to a gradual distancing from the Anglo-Saxon liberal philosophical tradition and its application to 19th century jurisprudence. Whereas investigative photojournalism would previously have affected only a small number of public figures and politicians, today the risk of improperly capturing and publishing private information is present at all levels of society. Big and small privacy snafus of the past few years have not only impacted celebrities. The need to manage one's digital traces now affects us all, as can be seen by the difficulties involved in applying the 'right to be forgotten' on a large scale.

22. Such a counter-history of the notion of the private sphere goes beyond the basic Hypothesis of the End-of-Privacy and the revisionist views that would make privacy a historical anomaly or even a null-and-void event. The care of privacy is the result of long-term cultural, political, and technological set of processes that are continuing in ICT-mediated social interactions. It fits neatly into our everyday working lives and usages, and reflects the structure of each of the operating social forces. It is closely linked to the democratic functioning and has proved indissociable from the gradual extension of civil liberties and their application to increasingly large swathes of the population. If in the past the requirement to protect privacy was not been perceived equally within populations, that was precisely because, as a concern, it is not immune to the influence of differential hierarchies and forms of subjection. The care of privacy is becoming more widespread insofar as modern democracies advocate – at least theoretically – a political space that is accessible to all. As Hannah Arendt would have it[27], it is the very possibility of accessing an active, professional and public, life that makes it necessary to draw a line between what pertains to collective achievements and what is confined to the individual's private sphere.

23. Although this possibility was previously restricted to a specific category of individuals (free able-bodied adult men with steady incomes), it now extends to all

[27] Arendt, Hannah (1958). The Human Condition. Chicago: The University of Chicago Press.

those (women, children, underprivileged citizens, etc.) who previously had no need to protect their privacy *precisely because they were excluded from public life.*

THESIS 4: PRIVACY HAS CEASED TO BE AN INDIVIDUAL RIGHT AND HAS BECOME A COLLECTIVE NEGOTIATION

24. Recent decades[28] have witnessed the establishment of a technological mediation over the right to a public life and, by implication, a private one. Active citizenship and the expression of the public will are achieved through the use of information and communication technologies. Online presence is therefore becoming a proxy for democratic participation. Far from leading to the erosion of the private sphere, this makes privacy an aspiration that is affecting the lives of an increasing numbers of persons around the world. Yet acknowledging this more widespread concern for private life, however important it may be in strengthening the argument against the Hypothesis of the End-of-Privacy, is not the same as saying that nothing has changed since the rapid rise of digital technologies.

25. We choose to describe the current transition as a shift *from privacy-as-penetration to a privacy-as-negotiation.*

26. The former approach takes us back to the 'right of the individual to be left alone' as set forth by Brandeis and Warren. It identifies a set of sensitive personal data (the 'privacies of life' referred to in a famous US ruling dating from the same period[29]) and places them at the heart of an individual space understood as a set of concentric circles of action. Such data would be 'private' by their very nature. This vision is based on a strict hierarchy of information, from more personal data that require greater protection to those that are less sensitive and are known by an ever-growing number of social stakeholders. According to this approach, there is therefore a set of core sensitive data that need to be protected, while the rest can easily be made public in line with a clearly unidirectional vision. An invasion of privacy is perpetrated by an external agent who manages to penetrate an individual's core sensitive data.

27. The concept of privacy as an individual right, insofar as it embodies a normative stance, represents an ideal situation that is barely recognizable in our day-to-day lives. It becomes a starting point from where to start factoring in new cultural sensibilities and technological advancements. Against a backdrop of social connectivity provided by digital devices, the intimate sphere of each individual cannot be composed in isolation. *No one wants 'to be left alone' on social platforms and yet everyone expresses a care of privacy that is specific to them*. In their everyday interactions, individuals endeavor to contribute actively either to disclosing or to keeping information secret, in order to limit intrusions from the outside and, more generally, to

[28] The following pages take up and develop the topics discussed in Casilli, Antonio A. (2013). Contre l'hypothèse de la fin de la vie privée. La négociation de la privacy dans les médias sociaux. Revue française des sciences de l'information et de la communication, 3 (1), http://rfsic.revues.org/630

[29] Boyd v. United States (1886) 116 U.S. 616

establish a set of rules and privileges for accessing specific aspects of their lives. By accepting or avoiding interactions and by adapting their frequency and intensity, individuals themselves adopt behaviors that are aimed, either explicitly or implicitly, at sorting all the information that could be the subject of social interactions in a dialectical and dynamical manner.

28. The increasing prominence of networked interactions empowers social stakeholders to display a strategic desire to create and maintain their areas of autonomy. In this new paradigm, privacy is not be construed as an individual prerogative, but rather a *collective negotiation*. It results from a relational arrangement that takes into account inter-subjective factors and is modeled around the signals received from those with whom an individual interacts. Privacy in online social platforms and in relationships mediated by mobile technologies is unique in that it is a decentralized, complex and multidirectional process.

29. Within ICT-mediated sociabilities, the social environment of each individual is not established in advance, but is supposedly defined by them. This situation, which typically arises when a user joins an online social network, requires above all that they evaluate the context in which interactions will take place (the participants, limits, norms, etc.) to be able to adjust the content of their communications. Building an online presence also requires users to protect themselves against intrusions from the outside, as well as managing the outgoing flow of data. To do this, each individual normally starts by a gradual disclosure of personal information that is intended to encourage feedback from the community of their interactors.

30. Unlike the traditional privacy-as-penetration model, none of the data shared are private, sensitive or intimate *per se*. All information is a signal sent by its author to their own environment, to the members of their personal online network. Because this signal aims to provoke a reaction from these members, the individuals help one another to adapt the information that they share by developing response and collaboration mechanisms. It is primarily by gathering this feedback and these evaluations – whether positive or negative – that users are able to establish, via trial and error, which data should be considered private and which can on the contrary be disclosed in a given context[30].

31. In that it is based on seeking an agreement between several parties rather than on a rule decreed by just one of them, this vision of privacy can be likened to a collective bargaining.

32. Stakeholders seek a consonance, compare their different interests and make mutual concessions in terms of disclosure and access to potentially sensitive information. The loss of privacy in certain areas is not equivalent to an uncontrolled debacle, but rather to a strategic withdrawal over subjects where negotiation proves challenging. It is through this collaborative disclosure accompanied by complex processes of selection and influence, that participatory surveillance is made possible—

[30] Cf Donath, Judith (2007). Signals in social supernets. Journal of Computer-Mediated Communication, 13 (1): 231–251.

and can eventually be surpassed. From a citizen's standpoint, mass surveillance programs cannot be countered by asserting an individual right to privacy as a sphere that resists all penetration, but rather by re-establishing a symmetry between the forces involved in this negotiation process: governments, markets, and users-citizens.

CONCLUSION: AGAINST THE 'PRIVATIZATION OF PRIVACY'

33. In the current political climate, defining the notion of privacy by emphasizing the aspects that make up the conflicting interests of various social stakeholders gives rise to a reaction that we should try to avoid – that of likening the 'negotiation' of privacy to its 'commercial exploitation'.

34. Privacy has undergone a transformation. It is no longer a transaction where each individual is alone against all others, but rather a collaborative process where the motivations of each citizen combine to create social collectives (such as advocacy groups, trade associations, and recognized bodies serving shared interests) engaging commercial organizations and governments in confrontations. The eminently collective nature of the current negotiation over privacy enables us to see its advocacy above all as an antagonistic and iterative conflict around the adaptation of rules and terms of service to users' needs. This process has been marked by a series of disputes and controversies that governments have had difficulty framing, in a generalized scheme involving the whole of civil society, owners of big data-processing companies and state intelligence agencies. No one doubts that this collective negotiation is inextricable from the protection of individual liberties, which must be enabled by specific legislation to counterbalance the bargaining powers between different stakeholders.

35. The existing legislative framework is still based on a privacy-as-penetration model and aimed to 'leave users alone' by interrupting communication flows and interconnections. It does not reflect the key demands of the citizens of an ICT-mediated society: to gain greater control over their own data through digital literacy, as well as through comprehensive citizen empowerment programs, and the introduction of infrastructures promoting the autonomy of communities of users.

36. Inevitably, this vision does not sit well with contemporary moves to apply the principles of private ownership to personal data, something that could be labeled as 'privatization of privacy'. Viewing privacy solely as an individual issue, or indeed as an infinitely monetizable and alienable asset, is sometimes presented as a way of making up for the commercial exploitation of personal data in which digital platforms and data brokers are already engaged. This is the argument put forward by commentators such as Jaron Lanier, who, while highlighting the inability of civil liberties to protect privacy in the age of the Internet, advocates the use of commercial rights through the introduction of a system of micro-royalties that Internet companies

would have to pay to users in order to collect, store and use their personal data for commercial purposes.[31]

37. Whether seen as a simple cultural provocation or as a dystopian vision, steps towards making this proposition a reality have so far been taken both by tech giants and by start-ups willing to experiment with offering remuneration to digital platform users in exchange for access to their data.[32] The World Economic Forum was already describing personal data as a type of emerging asset as early as 2011.[33] This classification, that would equate personal data to a 'repugnant market' (such as the trade in human organs or of citizenship rights), poses a problem for both legislators and citizens. Interestingly, some European countries have taken strong stances against these commercial practices. For example, in 2014 the French Council of State has deemed private ownership over personal data incompatible with the "right to informational self-determination"[34], while the National Digital Council (CNNum) has declared its opposition to applying private ownership rights to personal data. The main reason given, which is in line with the need to respect the collective nature of the negotiation of personal data, was to balance 'the power relationship between consumers and businesses'.

38. The sale of data under a private ownership system would generate only inconsequential incomes and would further foster socio-economic inequalities. Moreover, the framing of the current 'privatization of privacy' proposals, with their excessive focus on the commercial element, would do away with the role of governments as participants in this market, in their capacity as buyers of citizens' personal data for surveillance purposes.[35] With a private ownership system, citizens would be in even less of a position to defend themselves and their negotiating power would therefore be weakened.

39. These issues are destined to become only more pressing with the expansion of the Internet of Things. One of its immediate repercussions is the upsetting of the balance between the 'Internet of publication' (which includes contents voluntarily put online by users) and the 'Internet of emission' (which includes data and metadata transmitted by our smart devices, over which users have little or no configurating and negotiating prospects). To date, in this new paradigm consent to sharing personal data is largely assumed by default, on an opt-out basis, and has not been accompanied by any attempts to raise awareness and understanding of the related personal and social issues. The capture of data emitted by meters, electronics, and smart appliances

---

[31] Lanier, Jaron (2013). Who Owns the Future?. New York: Simon & Schuster.

[32] For example, companies such as YesProfile.com, Singly.com, Personal.com and Datacoup.com, which have made moves in this direction by offering users the opportunity to 'take back control and ownership of your personal data'.

[33] World Economic Forum (2011). Personal Data: The Emergence of a New Asset Class, http://www.weforum.org/reports/personal-data-emergence-new-asset-class

[34] Richard, Jacky & Laurent Cytermann (eds) (2014). *Op. cit.*

[35] Soghoian, Christopher (2012) The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance'. Phd thesis Indiana University.

installed in private homes, as well as by public transports and ambient components of urban infrastructure (sensors, cameras, etc.), is already a part of our everyday lives. However, it is destined to reach a critical point at which neither individual rights nor measures to protect the private ownership of personal data will be enough to counter the increasingly powerful forms of data expropriation to which citizens will be exposed. In the political context that is currently brewing, legislation based on individual rights would be nothing but a paper tiger.

40. Breaking free of the conceptual trap of the 'privatization of privacy' means both recognizing the dangers of reducing the elements that make up the connected lives of citizens to purely commercial assets, and the need to move away from the logic of personalized privacy, so that it can be envisioned as a collective concern, sitting within a framework that respects autonomy and liberties.