Tortious privacy 3.0: a quest for research

GIOVANNI COMANDÈ*
Scuola Superiore Sant'Anna

SUMMARY

This paper challenges the approaches typically employed to regulate data protection and privacy today. The paper emphasises the pitfalls of traditional notions such as 'anonymity' in modern technology-driven societies and aims at introducing a more comprehensive approach, termed Privacy as a Framework (PaF). In PaF, privacy remains at the centre of legal rules, shedding light on the interpretation of other core areas such as consumer protection or competition law. Also, the paper begins to explore some patterns for deregulation via private law and their implications in terms of 'privaticity', the abusive use of private information, as opposed to the traditional target of the civil liability for privacy infringement leading to 'ruthless publicity'.

1 INTRODUCTION: THE TENETS OF WARREN AND BRANDEIS IN THE INFORMATION SOCIETY

When Warren and Brandeis wrote their ground-breaking article[1] they were facing highly innovative technologies, for their time. They cried that 'recent inventions and business methods' (in their words, 'instantaneous photographs . . . and numerous mechanical devices') 'call for attention'.

They were taking up arms against the *use* of 'recent inventions and business methods' in dealing with personal data. Yet, the words 'personal data' or similar concepts or phrasing did not even appear in their seminal work. The closest reference was to personal gossip, productions, writings and appearance. Indeed, those prominent jurists were addressing the risks of 'ruthless publicity' of private facts, not the ruthless private use of private facts ('privaticity' as termed later in this paper).

A lot has changed since then. The dramatic expansion of the data-collecting and data-processing ability of both private and public entities is shifting (we hope) the attention from the fear of government as Big Brother[2] to the reality of multiple Big Brothers not necessarily aiming at control for political reasons but at developing the data economy. However, the basic issue dealt with in 1890 remains the same: the limits of collection and use of personal information by private and public players enabled by technological means, for both public and private interests.

What is different now is the incredible expansion of possibilities we are experiencing, enabling talk of 'data economy';[3] what is different is the immense good that reasoned use of personal data could produce and conversely the risks it entails.

* JD (Pisa) LLM (Harvard) PhD (Scuola Superiore S.Anna). Professor of Private Comparative Law at the Scuola Superiore Sant'Anna in Pisa and member of the European Group on Tort Law.

1 Warren and Brandeis 'The right to privacy' 1890 (4) *Harvard L Rev* 193.

2 Orwell *Nineteen Eighty-Four* (1949).

3 Worldwide Big Data Technology and Services – 2012–2015 Forecast, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6242.

As a matter of fact, the increase in the production, collection and processing of personal and sensitive data is paired with the evolution of the technologies for storing and processing (big) data, raising unprecedented privacy challenges and threatening to disrupt the already precarious trust users have in new technologies and public control over information.

Nevertheless, the immense difference between Warren and Brandeis' time and today is that surreptitious ways to collect and process data mostly triggered the peril of 'ruthless publicity' at their époque, while today they trigger what we might term 'privaticity', the use of private data for unperceived purposes that can lead to direct individual harm, indirect harm or simply to produce private or public gains. The ambiguity of this situation is reminiscent of the one faced in 1890 between lawful 'publication of matter which is of public or general interest' and 'the unwarranted invasion of individual privacy', but both private and public interests today present a larger impact on society and involved individuals.

However, the present day situation is the result of the ever-increasing adoption of the information society tools (mainly but not exclusively the Internet) and of mobile devices that allow for unobtrusive and cost-effective access to previously inaccessible sources of behavioural information, which could be protected as personal and sensitive data according to actual and forthcoming regulations[4] but still remain mostly a massive data production unperceived by most individuals. Health-related data is a prime example that is easy to understand, especially in those legal systems in which private health-care insurance is the main way of covering health-related risks.

In addition, modern technologies enable the identification of the data subject[5] even for data officially described as anonymous. For instance, it is enough to have four data points – approximate places and times at which an individual was sending a text or placing a phone call – to identify 95% of people in a given data set.[6] Indeed, officially anonymous or anonymised data are rather easily traceable back to individuals.[7] A similar process happens in the customary advertising we receive while using a mobile device or perusing the Internet on a computer: if we try to run an anonymous session on a browser we immediately realise that ads are still targeting us or, better stated, one of the identifiers loosely associated with some behaviours or with a collection of dispersed information gathered on the device in use (eg if one is in Italy and searching anonymously on an English web site, the device would most probably receive spatially aware advertisements in Italian).

Clearly the progressively more complex forms of online processing of personal data accentuate the problem of controlling the flow of personal information in the borderless cyberspace, and require a truly functioning ecosystem that provides demonstrable compliance with data

4 See the Proposal for a 'Regulation of the European Parliament and of the Council' on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

5 The identified or identifiable natural person whose personal information is concerned, according to the definition in art 2 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

6 De Montjoye, Hidalgo, Verleysen and Blondel 'Unique in the crowd: the privacy bounds of human mobility' 2013 *Nature SRep* 3, http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html. See also Article 29 Data Protection Working Party 'Opinion 05/2014 on anonymisation techniques', 0829/14/EN (10 April 2014).

7 De Montjoye, Kendall and Kerry 'Enabling humanitarian use of mobile phone data' 2014 (26) *Issues in Technology Innovation* 1, 3.

protection. Several regulations (either specific as in the USA or general as in the EU[8]) require public and private entities to abide by specific rules. But despite all the efforts, their effectiveness does not meet with expectations.

2 FROM 'PUBLIC' GOVERNANCE TO 'PRIVATE' DEREGULATION IN THE DATA ECONOMY

All the above happens against a backdrop of regulations that, while not averse to the recognition of privacy as related to fundamental rights or as a fundamental right in itself[9] (and not far from the personality approach of Warren and Brandeis), *de facto* enable ample commodification of personal data,[10] shifting the governing rules (at least apparently) from public regulation and principles enforced by authority to private deregulation via contract rules (term of service and privacy policies), and thus from public heteronomy to private autonomy.

Indeed, users are often formally called to make decisions concerning the disclosure of their personal information on the basis of a difficult trade-off between data protection and the advantages stemming from data sharing – for example, when interacting with smart-transport or health-care systems. Unfortunately, when data is collected by websites and mobile device apps, for instance, decisions on data use do not involve the identified or identifiable natural person whose personal information is concerned: clauses are consistently 'take it or leave it'.[11]

Terms of Service (ToS) and Privacy Policy Terms and Conditions (PPTCs) regulate the use of electronic devices, but they are normally not read[12] before accepting and the actual flow of data is often not even perceived by users since it runs in the background. For example, everybody realises that pre-installed apps[13] on ICT devices do not even allow activation of the apps themselves before consenting to the ToS and PPTCs, let alone the kind and extent of personal data collection and processing that they involve.[14] This process produces an effective

8 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

9 Again, the EU legal framework can serve as a suitable example followed in large parts of the world such as francophone Africa. See in general 'European Union Agency on Fundamental Rights', *Handbook on European Data Protection Law* (2014), https://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law.

10 Samuelson 'Privacy as intellectual property' 2000 (52) *Stanford L Rev* 1125; Elkin-Koren and Weinstock (eds) *The Commodification of Information* (2002); Prins 'Property and privacy: European perspectives and the commodification of our identity' in Guibault and Hugenholtz (eds) *The Future of the Public Domain, Identifying the Commons in Information Law* (2006) 223–257; Bergelson 'It's personal, but is it mine? Toward property rights in personal information' 2003 *UC Davis L Rev* 37, 379; Schwartz 'Property, privacy, and personal data' 2004 (117) *Harvard L Rev* 2055; Purtova 'Property rights in personal data: learning from the American discourse' 2009 25(6) *Computer Law and Security Rev*; Victor 'The EU General Data Protection Regulation: toward a property regime for protecting data privacy' 2013 (123) *Yale LJ* 513.

11 Nissenbaum 'A contextual approach to privacy online' 2011 140(4) *Daedalus* 32–48.

12 Bakos, Marotta-Wurgler and Trossen (2009) 'Does anyone read the fine print? Testing a law and economics approach to standard form contracts' *CELS 2009 4th Annual Conference on Empirical Legal Studies* 09-40. Indeed, it has been estimated that on average we would need 244 hours per year to read every privacy policy we encounter (see MacDonald and Cranor 'The cost of reading privacy policies' 2008 *Journal of Law and Policy for the Information Society* (2008 Privacy Year in Review Issue), http://www.is-journal.org).

13 Here, app is used as a synonym for software.

14 Lipford, Watson, Whitney, Froiland and Reeder (2010) 'Visual vs compact: a comparison of privacy policy interfaces', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA, ACM) 1111–1114; Passera and Haapio 'Transforming contracts from legal rules to user-centered communication tools: a human-information interaction challenge' 2013 1(3) *Commun Des Q Rev* 38–45.

deregulation output via private law that risks both twisting any active state intervention in the deregulation policy and outplaying fundamental principles.

The operational consequence is paradoxical but effective: can anybody explain why every app installed needs access to the full range of personal data present on the device in order to work? For instance, what is the need of an airline app for online check-in to have access to all pictures and addresses in the mobile device and on its location in time and space?

The answer is simple: it's the *data* economy, stupid! In other words, even when the business model of the software/app is not based on personal data collection it collects – and stores, shares, and sells – a large amount of information totally unrelated to the service it provides. The data subject easily loses track of this and remains unable to understand which data controller has provided her data to subjects the data subject does not want to share it with (see *infra*).

The fact that the service is in itself only saving money for the provider (eg costs of human or mechanised work for processing the check-in at the gate, making more efficient the use of vehicles, saving toner and energy for printing the boarding cards, etc) only adds insult to (personal data) injury by calling one's work their service.

3 THE ROLE OF 'UN-ANONYMITY' ON 'DATA PRIVATICITY'

Another relevant example is offered by big data associated with mobility and health issues, where new applications and smart devices are collecting daily users' personal and sensitive information through 'free' services without disclosing how data are processed, let alone used, at present and in the future.[15] Think for instance how interesting it would be for the insurance industry to know one's (un)healthy habits when it comes to renewal of one's individual healthcare insurance policy. Or think about the value to the automobile insurance market of being able to track down the speed of movement of one's mobile devices – gathered by mobile cells or Bluetooth antennae – as compared to the speed limits that are enforceable on the very roads the mobile is tracked moving on.

The last example leads us to another key point. Under any regulation presently in force, although questionable on legal and ethical grounds, it can be argued that the data might not be (or be perceived as) individual (human-related) data but as data of things. The mobile device with its unique identifiers is tracked down and there is no conclusive evidence to show that its owner was moving along with it. Yet, statistically it is a valuable clue about the owner's behaviour that might not even require justifications on the setting of insurance premiums. Indeed, even in the fully unfolded scenario of the 'Internet of Things', data of things is traceable to individuals either in a legally conclusive manner or at least in a statistically highly relevant way. In other words, the dubious data, whether they represent your dog running away with your mobile phone in its mouth or your crossing a red light with a car, might not lead to your liability for a fine but can still lead to a higher insurance policy premium without your knowing why the premium is escalating or how it came to be that the insurance company holds

15 The range of health parameters already covered by body sensors include stride length, distance from a specific location, step count, cadence and speed, heart rate, heart rate variability, heart rate recovery, respiration rate, skin temperature, skin moisture levels, breathing rate, breathing volume, activity intensity, body temperature, calories burned, distance travelled, sleep quality, sleep patterns, back posture, sitting position, chest and shoulder position, force of impact to the head (used in contact sports), exposure to the sun (UV measurement), biomechanical data collected while running, altitude and rate of ascent/descent, location (3D), motion parameters including speed and acceleration, repetitions of specific physical activities (eg sit-ups, dips, press-ups).

information about your device's routinely crossing red lights or speeding. Modern technology has un-anonymised anonymous data.

Although it is not the focus of this contribution, it can be claimed that those apps/programs mentioned above (eg the online check-in app) could easily switch to a business model that is privacy-minded, with enormous gains in terms of business appeal. However, the fact that this is not yet happening produces, for technology users at least, a lack of understanding of who processes their data and for what purpose it will be used, even assuming some sort of perception of the ongoing data processing is present and there is awareness of the economic value of data generated by users.[16]

While the above explains why an alternative market based on efficient privacy-friendly business models compliant with existing regulations has not been developed yet, it also shows the potential disruptive impact of such business models in which individuals are effectively offered the alternative to access services and use apps and software that enable them to successfully and measurably choose the level of data they want to share and with whom. Similarly the above examples illustrate the meaning of 'data privaticity', a use of private data which might even be in the grey zone of legality but clearly poses problems which the current privacy legal frameworks – even the more radical ones based on the extensive use of anonymous data as a default – fail to address properly. They also begin to illustrate the centrality of privacy for the regulation of other fields such as consumer protection, unfair business practices, and the like.

Actual knowledge and perception of both technical and business processes underlying data processing and their implications are key for such a different data economy that minimises 'privaticity' and maximises private and public gains from data sharing. While it was easy to perceive the intrusive potential of 'instantaneous photographs' used by others in 1890, modern technology users have the misled feeling that they control the device that generates data because they are using it.[17] However, this is not necessarily correct because, understandably, they are not familiar with the technological underpinnings of the technology they are using. Again, nobody understands the legal and technical reasons for airlines gaining such a widespread access to personal information, patently unrelated to the service provided and possibly amounting to an unfair business practice, yet we are unable to even install the app without providing such access.

In short, in the subtle commodification process of personal data[18] deregulating takes the form of contractual clauses or privacy policy declarations not known or fully understood, let alone providing accountability for actual data use.[19] At least, technical, legal and social implications of privacy settings remain difficult to comprehend for ordinary and even experienced

16 See 'User perspectives on mobile privacy' (September 2011). Indeed, terms are often barely readable let alone understandable to average users. See Black and Stanbridge 'Documents as "critical incidents" in organization to consumer communications' 2012 (46/3) *Visible Language* 246–281.

17 Users typically give their devices full rights to operate as if they were the users themselves. See eg Baldini *et al* 'A framework for privacy protection and usage control of personal data in a smart city scenario' in Luiijf and Hartel (eds) *Critical Information Infrastructures Security: Lecture Notes in Computer Science* vol 8328 (2013) 212–217.

18 See in general the sources cited in fn 10 above.

19 See in this regard Article 29 Data Protection Working Party 'Opinion 3/2010 on the principle of accountability', 00062/10/EN, WP 173, 13.7.2010; ID 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union"' *Official Journal of the European Union* C 181, 22.6.2011, 1–23.

users.[20] These problems become more acute for data collected in the background as apps are used across private and public settings. For regular users it is virtually impossible to follow and track what is shared among multiple databases matching different device identifiers[21] with other personal data and how this is done.

The above state of art, along with disparate regulations across legal systems, might adversely affect the social value of wider use of personal information for public and private benefit. Were the trust in data-sharing technologies lost, the opportunities in exploiting personal and sensitive data to enable new generations of person-aware applications to use data in the public benefit (eg in pandemic risk detection and containment, or for use in disaster emergency situations[22]) might be lost forever.

Thus, in a context of extensive 'privaticity' and ineffective anonymity, whatever understanding of data economy is endorsed and used, the need clearly emerges to move from *privacy as an addendum* to other regulation (a mere set of constraints in using data to protect the individuals' privacy) towards a new concept of *privacy as a framework* for all other forms of (private and public) regulations.

4 FROM REGULATING PRIVACY TO PRIVACY AS A FRAMEWORK

The data economy offers many advantages for enterprises, users, consumers, citizens and public entities. Its multiple manifestations, such as the web of social networks and the so-called Internet 2.0, the Internet of Things, provide unprecedented scope for innovation, social connections, original problem solving and problem discovery (eg on emerging risks or their migration patterns such as in pandemic emergencies).[23] All these require the gathering and processing of data on both devices and individuals that raise conflicting concerns (maybe not enough or even exaggerated ones at times[24]) between, on the one hand, the will to share and participate (in social networks, for instance, or in public alerting systems in the case of natural disasters) and, on the other hand, the apprehensions about the reliability of the organisations involved[25] that go well beyond the 'Snowden affair' and the WikiLeaks approach.[26]

20 See 'User perspectives on mobile privacy' (September 2011).

21 Hartzog 'Website design as contract' 2010 *Am UL Rev* 60, 1635; Hartzog and Stutzman 'Obscurity by design' 2013 *Wash L R* 88, 385.

22 See De Montjoye and Kendall 'Enabling humanitarian use of mobile phone data' 1ff; Villasenor 'Smartphones for the unbanked: how mobile money will drive digital inclusion in developing countries' 2014 (25) *Issues in Technology Innovation* 1ff.

23 Wesolowski, Eagle, Tatem *et al* 'Quantifying the impact of human mobility on malaria' 2012 *Science* 338 (6104) 267–270; Wesolowski, Buckee, Bengtsson *et al* 'Commentary: containing the ebola outbreak – the potential and challenge of mobile network data' 2014 *PLOS Current Outbreaks*; Bengtsson, Lu, Thorson *et al* 'Improved response to disasters and outbreaks by tracking population movements with mobile phone network data: a post-earthquake geospatial study in Haiti' 2011 8(8) *PLoS Medicine* e1001083.

24 Phelps, Nowak and Ferrell 'Privacy concerns and consumer willingness to provide personal information' 2000 19(1) *Journal of Public Policy & Marketing* 27–41.

25 Pew Research Centre 'Mobile Health 2012', Pew Research Center's Internet & American Life Project (2012), http://pewinternet.org/Reports/2012/Mobile-Health.aspx; Benenson, Gassmann and Reinfelder 'Android and iOS users' differences concerning security and privacy' *CHI '13 Extended Abstracts on Human Factors in Computing Systems* (2013) 817–822; Buttle and Burton 'Does service failure influence customer loyalty?' 2012 1(3) *Journal of Consumer Behaviour* 217–227; Wood and Neal 'The habitual consumer' 2009 19(4) *Journal of Consumer Psychology* 579–592.

26 For a summary of the approaches and problems raised by the processes started by Edward Snowden and WikiLeaks see Klein 'Wikileaks, Arab uprisings, English riots and occupy Wall Street: implications for Internet policy and practice from a business and industry outcome perspective' (18 September 2011) 2012

The exponential growth of interactive, context-sensitive mobile devices along with (supposedly) user-aware interactions with service providers in the domain of transportation and health-care or personal fitness, for instance, dynamically generate new sources of information about individual behaviour or, if you wish, the behaviours of their devices, including personal preferences, location, historical data and health-related comportments.[27] Based on mobile cells, using Wi-Fi connections, GPS sensors, Bluetooth, et cetera, several apps use location data to provide 'spatial aware' information. They allow users to check in at specific locations or venues, to track user movements and outdoor activities and then allow the user to share this kind of information.[28] Modern devices are either developed or under development with health-state measurement and monitoring capabilities being incorporated in the device itself or provided through external devices in the form of smart watches, wearable clips or bands. The information provided can be employed for health care, for personal fitness, or in general for obtaining measurable information as part of quantified own practices that lead to marvellous potentials both in public and private use but also raise concerns and the need to implement a clear technologically neutral regulatory framework that moves from privacy and relates to all legal fields involved,[29] empowering a more balanced dealing between individual data subjects/users and organised data controllers.

The above-mentioned kind of data constitutes individual and social assets of enormous relevance that require a comprehensive approach. Nevertheless, the traditional approaches to privacy conceived as one piece of a multifaceted and unrelated puzzle of regulations do not offer such a comprehensive approach because they miss the link between social and economic needs, law and the technological implementation of legal rules. They neglect also to take fully into account the actual functioning of specific devices and the general trends of technology, failing to embed effective protection in existing legal data control tools (privacy as a fundamental right) and the eventual need/opportunity to introduce *sui generis* forms of proprietary protection (personal data as commodities) in a framework of high users' abilities in governing their personal data.

Recently the need for change has been stressed. The World Economic Forum has launched several initiatives under the 'Rethinking Personal Data' project, which brought together different sets of stakeholders with the aim of offering a comprehensive overview of the state of the art in data usage and protection, and of developing a collaborative and principled ecosystem to unlock the value of personal data while fostering consumer trust and protecting their fundamental rights. The reports shed light on industry dynamics, selected consumer needs and

(14.6) *Information, Communication & Society Journal*; Karatzogianni and Robinson 'Digital Prometheus: WikiLeaks, the state–network dichotomy, and the antinomies of academic reason' 2014 (8) *International Journal of Communication* 2704–2716.

27 Elkin-Koren and Weinstock (eds) *The Commodification of Information*; FTC 'Mobile privacy disclosures: building trust through transparency', FTC Staff Report (Feb 2013), http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; FTC 'Mobile apps for kids: current privacy disclosures are disappointing', FTC Staff Report (Feb 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; FTC 'Mobile apps for kids: disclosures still not making the grade', FTC Staff Report (Dec 2012), http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; Canadian Offices of the Privacy Commissioners 'Seizing opportunity: good privacy practices for developing mobile apps' (Oct 2012), http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf; Harris 'Privacy on the go: recommendations for the mobile ecosystem' (Jan 2013), http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

28 See 'User perspectives on mobile privacy' (September 2011).

29 Sundsøy, Bjelland, Iqbal *et al* 'Big data-driven marketing: how machine learning outperforms marketers' gut-feeling' in Greenberg, Kennedy and Bos (eds) *Social Computing, Behavioral-Cultural Modeling and Prediction* (2013) 367–374.

interesting public initiatives, and elaborated different public and private policies to strike a balance between opposite interests.[30]

Against this background technological and legal solutions remain widely unrelated to each other. Despite having been enacted in the mid-90s when the Internet was already in existence, end-user data protection is dominated by a legal privacy-by-policy approach.[31] Its notice-and-choice implementation strategy is supposed to provide users with information on how personal data is processed in a comprehensive manner, allowing for informed consent to it. Even the radical alternative to provide end-user privacy by default, that is by not processing identifiable personal data above the level of necessity (a strategy originally embedded without much success in article 3 of the Italian data protection law 196/2003[32]) has proven not very effective both because it was rarely implemented and bent by the above-noted private deregulation.[33]

This rather recent attempt to answer the general problem of information privacy with privacy-by-design architectures[34] fails as well. Although rightly building on the philosophy and methodology of embedding privacy into the design specifications of information technologies, business practices and networked infrastructures as core functionality, it is no longer sufficient to deeply and meaningfully embed respect for privacy across public and business organisations. Privacy-by-design architectures run the risk of undermining public and private uses, which might be of high value while of low or non-existent risks for data subjects. Indeed their approach fails to take fully into account the evolution of the key notion of anonymity that remains at its main core. For example, granting anonymity by allowing a user to be unidentifiable in a group of other users,[35] proves increasingly fallacious for the technical reasons explained above and jeopardises the ability to exploit the data for public benefit without offending the rights of the data subjects.[36]

For more than two decades scholars have been focusing on the 'commodification of identities and behaviours'[37] caused by the advent of new technologies. Several contributions have already emphasised the great divide between the EU command-and-control and the US market-oriented approach to personal data, and have long debated the pros and cons of the privacy-

30 The reports are available at http://www.weforum.org/issues/rethinking-personal-data.

31 Spiekermann and Cranor 'Engineering privacy' *IEEE Transactions on Software Engineering* (January/February 2009), http://ssrn.com/abstract=1085333.

32 See also European Union, Directive 95/46/EC, Recital 26.

33 See 1 above and accompanying footnotes.

34 See Cavoukian 'Privacy by design . . . take the challenge' (Jan 2009), http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf; *Privacy by Design* Resolution, 32nd International Conference of Data Protection and Privacy Commissioners, 27–29.10.2010, Jerusalem, http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf; Article 29 Data Protection Working Party 'Opinion 3/2010 on the principle of accountability', 00062/10/EN, WP 173, 13.7. 2010; 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union"', *Official Journal of the European Union* C 181, 22.6.2011, 1–23; Lessig 'Code 2.0', http://codev2.cc/download+remix/Lessig-Codev2.pdf; Schaar 'Privacy by design' 2010 3(2) *Identity in the Information Society* 273; Spiekermann and Cranor 'Engineering privacy'.

35 In the USA eg lists of data to be stripped for producing anonymity are produced but again without much success when facing modern computing ability. See eg the privacy rule issued by the American Department of Health and Human Services to protect the privacy of patient health records (45 CFR 164.514). See also Gedik and Ling 'Protecting location privacy with personalized k-anonymity: architecture and algorithms' (Jan 2008) 7(1) *IEEE Transactions on Mobile Computing* 1–18.

36 See De Montjoye, Kendall and Kerry 'Enabling humanitarian use of mobile phone data'.

37 Prins 'The propertization of personal data and identities' Oct 2004 8(3) *Electronic J of Comp Law*.

as-fundamental-right interpretation versus the privacy-as-property model.[38] Yet no conclusive result has been reached.

We claim here that a more radical change is needed: a switch to 'privacy as a framework'. Privacy as a framework would *overcome alternative views that contrast privacy as a fundamental right and as a commodity*.[39] It would enable clear choices distinguishing those related to data as an asset and those related to personal information affecting fundamental rights. The privacy-as-a-framework approach would overcome the dualism of information privacy as a fundamental right contrasted with privacy reduced to a business opportunity. Such a radical change of paradigm is mature in modern societies based on a data economy, a change that puts privacy as a framework at the centre. For instance, both mentioned regulatory models are *de facto* based on an 'informed consent' ability to unlock every form of data processing. Yet, both models fail to take into account the impact of technologies on processing ability and on the actual notion of anonymity.

Even without changing the actual legal rules on privacy, it is necessary to explore the potential interplay between the fundamental principles of privacy law and other legal rules such as unfair practices, competition and consumer protection. For instance, although it may be based on individual consent, a practice that in reality makes it difficult for users to be aware of what data processing they are actually consenting to might be suspicious under any of the previously mentioned sets of legal rules. Business models and practices that segregate customers in a technically unnecessary way (eg, offering asymmetric Internet connections to business and non-business clients), directing some categories to use the services in certain ways that make data collection easier and more comprehensive (eg through concentrated cloud-based services) might appear suspicious under another set of regulations once privacy as a framework illustrates their factual and legal implications.

Indeed, it is the very same volatility of the ICT field, where new services, interfaces and devices with a wide variety of applications and services are continuously emerging, that requires a change of framework able to tackle the reluctance of industry and regulators to take up recommendations and legal constraints.

'Privacy as a framework' requires a reclassification of legal rules related to privacy along innovative lines. Such an approach would influence and inform the entire regulatory framework for both public and private activities, overcoming the pitfalls of an approach that maintains separate rules, for instance, on data protection, competition, unfair practices, civil liability and consumer protection.

5 SOME HINTS FOR FURTHER RESEARCH

We have illustrated in the previous paragraphs that key technological innovations, along with the emergence of business models and practices, have the potential of frustrating the aims of privacy protection regulations across the existing different models. The paper has also claimed

38 *Ibid*; Litman 'Information privacy/information property' 2000 (52) *Stanford L Rev* 1290; Lessig 'Privacy as property' 2002 (69) *Social Research* 1, 255; Cohen 'Examined lives: informational privacy and the subject as object' 2000 (52) *Stanford L Rev* 1390; Samuelson 'Privacy as intellectual property' 2000 (52) *Stanford L Rev* 1125; Elkin-Koren and Weinstock (eds) *The Commodification of Information*; Prins 'Property and privacy: European perspectives and the commodification of our identity' in Guibault and Hugenholtz (eds) *The Future of the Public Domain, Identifying the Commons in Information Law* (2006) 223–257; Victor 'The EU General Data Protection Regulation: toward a property regime for protecting data privacy' 2013 (123) *Yale LJ* 513. See also the sources cited in fn 10 above.

39 See Elkin-Koren and Weinstock (eds) *The Commodification of Information*.

that ('informed') consent-based regulatory approaches encounter significant problems in these new contexts, leading to private deregulation that barely leaves users with any form of legal protection. Finally, the analysis has illustrated the impact of a notion of anonymous data profoundly changed by technology.

The above analysis leads us to call for a change in paradigm that puts privacy as a framework of reference for a wide range of regulations and as a key interpretative tool. Although the aim of this paper is not to fully illustrate how this change of paradigm could be pursued, it is worth illustrating some potential patterns that can be followed in further reflections.

Need we say that the underlying assumption is that data economy and data processing are not evil *per se*? On the contrary, the privacy as a framework paradigm acknowledges and cherishes data circulation as a mode of creating new opportunities and wealth for all in societies. It acknowledges the need to empower data subjects to exercise a larger degree of control over the flow of information and to expand the beneficial public use of data processing without impairing the benefits of free private use in a clear framework of rights and duties. In this dimension, rights and duties can assume unprecedented specific characteristics.

In the privacy-as-a-framework paradigm all these require the definition of a legal approach with various innovative characteristics able to foster actual competition, technological neutrality and freedom of choice.

The following characteristics are worth exploring.

5.1 Rights without duties

The acknowledgment in the proposed new EU data protection regulation of both the right of data portability and the right to be forgotten might not require duties directly enforceable by data subjects. What data subjects might need would be procedural rights capable of empowering effective comparison of services and changes of providers for virtually no cost.

5.2 Duties without rights

Conversely, the switch in attention from the right to avoid 'ruthless publicity'[40] to the risk of privaticity might lead to the implementation of duties on providers and data controllers that emerge from other legal fields (eg competition, consumer protection, unfair practices, etc) and do not immediately create enforceable rights for data subjects. It might be, for instance, the acknowledgment as abusive, unfair, anti-competitive, and the like, of actual practices or even entire business approaches. Indeed, in the past antitrust law has disrupted solid monopolies such as in the American telecommunications industry.

Such duties could not be enforceable by individual data subjects but authorities could enforce their compliance using a variety of mechanisms.

Since full and reliable anonymity is not technically possible, it might be useful to sustain procedural anonymity, strictly enforced by authorities and watched over by tort law. Indeed, such duties related to procedural anonymity (that is, access to data only under certain conditions) if violated, could be enforced *ex post* with liability rules and\or other sanctions. This procedural approach to anonymity would preserve the potentially immense benefits of public use of big data in scientific public infrastructures for sharing meta-data.

Alternatively, those duties might be enforceable by individuals in legal fields other than privacy law (such as unfair practices) but using privacy protection as interpretative tools to read

40 See Warren and Brandeis 'The right to privacy' 1890 (4) *Harvard L Rev* 193.

the old regulations. Yet the possibility of making them directly enforceable as privacy-related rights remains worthy of exploration.

5.3 Tort liability as a watchdog

Legal history teaches us that tort liability has been a flexible instrument of legal innovation. Although a remedy acting *ex post*, it has often had the ability to arrive first in offering legal protection to new legal interests or against new ways of offending legally protected interests. Indeed the birth and evolution of the tort of privacy or similar solutions is in itself a good example. Tort liability, along with contractual liability for unfair dealing and bad faith, might still remain useful legal tools to provide legal protection without stifling innovation.