International Data Privacy Law Advance Access published August 27, 2015

Cloud-enabled technologies and privacy paradigms: Israeli challenges and responses

Arye Schreiber*

Introduction

Almost all of the already vast literature on privacy in the cloud has focussed on the technicalities and problems of applying existing privacy law—legislation and case law— to a new technological reality. For example, legal scholarship of cloud computing has dealt with such vexing problems as discovery,[1] evidence,[2] inheritance and intestacy of digital assets,[3] conflict of laws and applicable jurisdiction,[4] data processing,[5] government access,[6] healthcare data,[7] and much more. Here, the focus is rather on whether and how the emergence of the cloud-enabled technologies is changing privacy; does the law have the tools to respond? And how is it to do so? As the question suggests, I believe these technologies are changing the ways in which our privacy is challenged. This article will address these issues with a particular emphasis on Israeli law, with some comparison to pertinent US case law. This article will focus on challenges to existing privacy law, and some steps available or already taken, particularly by Israeli law, to address these challenges.

Key Points

- Emerging technologies, especially cloud-enabled technologies, create new challenges to privacy.
- Privacy has widely been viewed as a matter of control of personal information.
- Cloud technologies threaten privacy as a part of one's sense of self, rather than control per se.
- Existing privacy torts do not adequately address new forms of injury. Two examples are discussed.
- One example: Data surveillance causes real injury even to a person who is not actually the target of the dataveillance, but that injury is not protected.
- Second example: Information manipulation is becoming increasingly prevalent and is a real but at present inactionable form of harm.
- A third and final area affected by cloud-enabled technologies is the horizontal–vertical divide. Privacy law in these two areas has distinct laws and treatment, but the lines between them are fast breaking down.

From sense of control to sense of self

One of the emerging challenges to privacy is that consumers and citizens in general lose control of their data,[8] and this has also been identified as such by the Article 29 Working Party Opinion on Cloud Computing:

> Despite the acknowledged benefits of cloud computing in both economic and societal terms, this Opinion outlines how the wide scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient

* Arye Schreiber, Schreiber & Co—Privacy and Cyber Law, 12 Hamaapilim, Jerusalem 9358801, Israel.
Email: info@schreiberlaw.co

1 C Pham, 'E-Discovery in the Cloud Era: What's a Litigant To Do?' (2013) 5 Hastings Sci. & Tech.L.J. 139.

2 J Dykstra and D Riehl, 'Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing' (2012) 19 Rich.J.L.& Tech. 1; P Ohm, 'The Future of Digital Evidence Searches and Seizures: The Fourth Amendment in a World without Privacy' (2012) 81 Miss.L.J. 1309.

3 M Perrone, 'What Happens When We Die: Estate Planning of Digital Assets' (2012) 21 IJCLP 185.

4 V Narayanan, 'Harnessing the Cloud: International Law Implications of Cloud-Computing' (2012) 12 Chi. J. Int'l L. 783.

5 W Kuan Hon, C Millard, and I Walden, 'The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated? The Cloud of Unknowing' (2011) 1 IDPL 211, and Part 2 of the same article (2012) 2 IDPL 3.

6 C Soghoian, 'An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government' (2011) 12 Minn. J. L. Sci. & Tech. 191.

7 'Healthcare Cloud Computing (Clinical, EMR, SaaS, Private, Public, Hybrid) Market—Global Trends, Challenges, Opportunities & Forecasts (2012–2017)' (July 2012) <http://www.marketsandmarkets.com/Market-Reports/cloud-computing-healthcare-market-347.html> accessed 19 May 2015.

8 JP Kesan, CM Hayes, and MN Bashir, 'Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency' (2013) 70 Wash.& Lee L.Rev. 341, 363.

> information with regard to how, where and by whom the data is being processed/sub-processed.[9]

As one author put it: 'The heart of the privacy issue with regard to cloud computing is the fact that you are handing over potentially highly sensitive and private information to a third party to store and process.'[10] For example, consumers are typically locked in to cloud SaaS providers, with little opportunity for migration to another service; on all aspects of security and data protection, consumers are almost entirely at the whim of the provider; and providers generally are able to shift the entire risk of loss to the consumer. On top of those, consumers have essentially no bargaining power to amend those weaknesses.[11] All this means that, to advocates of 'privacy as control', the cloud represents a battleground on which the starting premise is a substantial loss of privacy. Certainly, a large part of the loss of control over data is more perceived than real, or at the very least it is easily cured; even informed computer users are often unable to effectively manage their browser privacy controls, and very common technologies, such as Flash, allow those controls to be bypassed[12]; and as cloud service providers increase the user-friendliness of their services, and as consumers become better informed and as larger customers assert themselves in negotiation with cloud providers, we can expect users—both companies and individuals—to reassert some measure of control.[13] Still, Tene and Polontsky note that 'Privacy and data protection laws are premised on individual control over information and on principles such as data minimization and purpose limitation'.[14] This premise is fast becoming undermined, and the control paradigm is becoming dated. In the meantime, improved user-controls over data are a relatively obvious avenue to enhancing control over data, and we can expect to see cloud providers offer additional controls, perhaps as a premium, paid-for part of their business model.

However, while many sections and provisions of privacy law will be shaken by the change in the way data are controlled, this is not where new technologies will most challenge privacy law generally, and Israeli privacy law specifically—of particular interest to this author. In seeking to identify where the cloud most challenges privacy, we can draw inspiration from Citron's observation that 'insecure databases impact people's sense of self'.[15] Insecure databases undoubtedly do that, and so do other emerging phenomena in the world of privacy. The emerging threats to the sense of self, to the inviolate personality, are new and evolving, and it is to them that we now turn.

Inviolate personality cloud-enabled technologies: observation and manipulation

Since Warren and Brandeis popularized it, Cooley's definition of privacy as the right to be left—or let—alone[16] has been the most enduring definition or summary of privacy. Friedman rightly notes that new media have 'a profound effect on privacy, at least in the sense of being alone or being left alone'.[17] The right to be let alone, as Citron wrote:

> honors human dignity by conferring 'respect for individual choice' and 'respect for individuals because they have the capacity for choice.' It encourages creativity and self-development. Privacy provides a space for people 'to make up [their] minds and to develop new ideas' and fosters social relationships. Permitting individuals to form their personalities free from unwanted interference promotes selfhood and human relations, furthering a free society.[18]

Published in 2010, Citron's excellent article called for privacy torts to be brought within the general tort rubric. In particular, à la Citron the harm resulting from invasions of privacy is magnified by technological developments, and damages for invasions of privacy are more considerable and measurable than they were in the past. Indeed, the change in the scope and duration of invasions of privacy following from new technologies, as well as additional innovation and the resulting ways it can affect our behaviour, amount to novel forms of invasion of privacy. This is true not just in terms of the harm, and its measurability, but in substance as well. In particular, invasions of privacy and the resulting harm are not just magnified by technology; rather, there are forms of

9 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing 17, (EC) No. 01037/12, WP 196 (1 July 2012) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf> accessed 19 May 2015.

10 AC DeVore, 'e-Legal: Privacy and Law Enforcement on the World Wide Web: Cloud Computing: Privacy Storm on the Horizon?' (2010) 20 Alb.L.J.Sci.& Tech. 365, 371.

11 Ibid, see 426 and 427

12 P Lanois, 'Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?' (2010) 9 Nw. J. Tech. & Intell. Prop. 29.

13 W Kuan Hon, C Millard, and I Walden, 'Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now' (2012) 16 STLR 81.

14 O Tene and J Polonetsky, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 STLR Online 63, 67.

15 D Citron, 'Mainstreaming Privacy Torts' (2011) 98 CLR 1805, 1853, citing Leslie Meltzer Henry 'Spheres of Dignity' (unpublished).

16 SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4 Harv.L.Rev. 193, 195.

17 Lawrence M Friedman 'Guarding Life's Dark Secrets' (Stanford University Press, Stanford, CA 2007) pp. 258–9.

18 Citron (n 15), 1831–3, footnotes omitted.

invasion of privacy made possible by technological innovation that were not previously possible. In some jurisdictions, express legislation will be required to adequately address these emerging forms of damage; in others, this will be solved with small evolutionary steps (such as by case law in common law systems). Without diverging into the important discussion of how exactly different jurisdictions ought best to address these damages, I here discuss two of these as yet unaddressed or inadequately addressed forms of invasion of privacy: data surveillance and information manipulation.

Data surveillance

People's right to solitude has been a principle of common law for centuries. Particularly with reference to the home, it has long been law that 'the house of everyone is to him as his castle and fortress'. That sentence continued in the original as follows: 'as well for his defense against injury and violence, as for his repose'.[19] The protection of physical, virtual, and emotional space in which people can not only be secluded from prying eyes and ears, but also enjoy 'repose', develop their personalities and relationships is what we call privacy, and as Citron shows that it is this space that is increasingly at risk in an online world.[20]

As an illustration of the way in which perpetual surveillance and dataveillance affect our behaviour, consider the 'Hawthorne Effect', the appellation given in the 1950s by Henry Landsberger to the effect he observed in workers at the Hawthorne Factory; namely, that their behaviour changed when they were observed.[21] The same phenomenon has a long history in anthropology and psychology, where researchers and therapists attempt to observe without necessarily affecting the observed. This in a nutshell is the ultimate harm engendered by the spread of data surveillance, by rich data being collected about us all the time, and by behavioural analysis in every service we use: the more we are surveilled, observed, and recorded, the more our behaviour is affected. Nissenbaum has neatly summarized how increasing dataveillance affects our freedoms of inquiry, association, and expression:

> The function of the Web as a venue for commercial transactions, forming and maintaining associations, socializing, participating in political activities, and finding community with others, including a religious community, continues to increase dramatically. In relation to all these activities, common sense, endorsed by claims and findings of a vast literature on surveillance, affirms a connection between confidentiality and freedom. Specifically, the freedom to inquire, associate, and express . . . flourishes in an environment insulated from external scrutiny, secure against reprisal, interference, intimidation, influence, control and even embarrassment.[22]

Clearly sensitivity to surveillance is cultural, as different cultures react differently to being observed. By way of illustration, one author wrote over three decades ago that 'Americans are more reticent than Europeans when it comes to eye contact, the most extreme form of which is staring. Americans are brought up to think that it is rude to stare. In Europe, on the streets, in cafés, in other public places, staring is common and, indeed, represents one of the more intriguing accompaniments of a brief stop for refreshment at an outdoor café'.[23] This quaint and rather romanticized view of Europeans sitting around cafés staring at passers-by may not be accurate, but it highlights that at least part of the staring taboo is cultural, and that this is a reflection of different cultural perceptions of observation. Though sensitivity may differ, wherever human dignity is valued, there is a need for people to have space in which they may act, think, and develop unencumbered and unobserved, and to the greatest extent possible, uninfluenced.

Conversely, there is considerable evidence that our privacy is impinged simply by being observed, and even by the subjective feeling of being observed.

> So what is the value of privacy? Privacy creates a framework that allows other values to exist and develop. Where privacy is available, we can have freedom, liberty, and other intrinsic goods. We can develop friendships, relationships, and love. As anyone who has had a camera pointed at them knows, we act differently when being recorded. Now consider that everything we do online, over the phone, or with a credit card can be monitored and recorded. If this information is used abusively, similar to how we might feel if we were filmed all the time, it compromises our ability to act naturally and freely.[24]

As Sundquist noted, having 'a camera pointed' at one is disconcerting, and that is true even if the camera is not recording.[25] Though there is additional harm in being recorded with all the potential that has for further

19 *Semayne's Case* 77 E.R. 194, 195, per Coke C.J.

20 Citron (n 15), 1884.

21 Henry A Landsberger, 'Hawthorne Revisited: Management and the Worker, Its Critics, and Developments in Human Relations in Industry' (Cornell University, Ithaca, NY 1958). Landsberger's methods and findings have been subjected to considerable scrutiny and criticism, none of which is relevant for the present purposes.

22 H Nissenbaum, *Privacy in Context* (Stanford University Press, Stanford, CA 2010) 197.

23 MH Levine, 'Privacy in the Tradition of the Western World' in WC Bier (ed), *Privacy: A Vanishing Value* (Fordham University Press, NY 1980) 3, 5.

24 M Sundquist, 'Online Privacy Protection: Protecting Privacy, the Social Contract, and the Rule of Law in the Virtual World' (2012) 25 Regent Univ.L.Rev. 153, 158, footnotes omitted.

25 Discussed in more detail in A Schreiber, 'Through the Looking GLASS: Google Glass, Privacy and Opacity, with an Israeli law twist' (2014) 4:1 IDPL 69, 82.

damage, there is also harm inflicted from the feeling of being watched irrespective of the resulting data being abused. Data protection regulations—such as the Israeli Protection of Privacy Law 5741-1981 (the 'Privacy Law') and the European Data Protection Directive 95/46[26]—are focussed on regulating data controllers, processors, etc., and are intended and designed to prevent the misuse of personal data. Many people are concerned about misuse of their data, and these and other regulations reflect a desire not to allow someone who has my data to do with it as they please. The pervasiveness of data collection and analysis, and the exponential growth in data uses, mean that quite irrespective of any potential misuse, the relentless collection of data itself has a direct effect on our behaviour. Yet with the ascendance of cloud-enabled technologies, the fundamental premises of privacy harm are shifting. We have already to a dramatic extent relinquished control over our data, and though control remains important—as noted above—a much greater challenge today is how our behaviour is affected by moving our activities and data online.

Here, an important distinction must be made. In a sense, privacy has always been about how surveillance and interference in its many forms affect the victim's behaviour. The concern typically was two-fold; one level of concern was with the harm, quantifiable or otherwise, that would flow from an invasion of privacy, and this is largely economic harm; the other was the chilling effects that interference could have on a person's behaviour, which is particularly in the realm of emotional harm. Clearly, the latter ultimately evolves into the former, if not in any particular case, then at a societal level. In other words, a person may interfere with my private information, and in a given instance that may have no economic harm in itself, for example, if someone published my medical records. Yet if medical records were regularly violated, that would have serious ramifications for individuals, and more so for society. People may stop seeking psychiatric help because of the stigma attached to it. Or, they will avoid medical treatment for sexually transmitted diseases or other infectious diseases. For example, if a person's lawful political, financial, or health information is exposed, then that would be harmful to them in that it is a violation of their personality for these intimate details to be shared, and it would be harmful to society since it prevents people from pursuing these activities. Even if a given instance of revelation may not be harmful, knowing that private information is not protected will cause people not to consult health professionals and preserve their health, not to trust banks and take credit, and not to associate with political and values-driven institutions and improve society.

This is a common theme in privacy's many forms, and an entire branch of privacy law in the US constitutional privacy law is premised on the 'penumbras' and 'emanations' of privacy in the Constitution all of which point at the value to society of leaving the government outside of various areas of behaviour and activity. Specifically, *Griswold*[27] found privacy lurking in the shadows of the Constitution, making anathema the notion that the state may interfere in my thoughts, actions, personality, etc.

> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance... Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.
>
> The Fourth and Fifth Amendments were described in Boyd v. United States... as protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life.' We recently referred in Mapp v. Ohio to the Fourth Amendment as creating a 'right to privacy, no less important than any other right carefully and particularly reserved to the people.
>
> We have had many controversies over these penumbral rights of 'privacy and repose.'... These cases bear witness that the right of privacy which presses for recognition here is a legitimate one.[28]

There has been tremendous controversy over *Griswold*'s finding of privacy penumbra. The US Constitution nowhere mentions privacy, and many have argued that that Supreme Court of the United States has basically made up a constitutional right. But the 'zones of privacy' recognized by the court in that seminal case highlight

26 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.

27 *Griswold v Connecticut* 381 US 479 (1965).

28 Ibid, 484 and 485, per Douglas J.

people's need and the Constitution's recognition of the need of people to have those zones of privacy, areas in which the state and others may not interfere.

Privacy à la *Griswold* is constitutional, not tortious. No damage needs to be shown for an action under the *Griswold* doctrine. The very fact that the state impinges on my decision-making violates my constitutional rights, irrespective of any actual damage. The differences between horizontal and vertical privacy are further elaborated on below; here, we may look to *Griswold* for inspiration in seeking a re-evaluation of the actionability of dataveillance. Specifically, *Griswold* stood for the notion that there are areas which the state ought not to concern itself. Various rights or values, such as privacy, underlie constitutional provisions, and the court extended the technical provisions based on the underlying rights. This is a majestic piece of purposive constitutional jurisprudence; the court saw various constitutional rights as emanations of the constitution's value of privacy and repose, and the court therefore found that other legal protections of privacy and repose ought to have constitutional law status. One particular aspect of *Griswold* deserves attention here, namely that—as the *Griswold* court cited from *Boyd*[29]: 'It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property. . . .'[30] The court recognized that there are actions that will violate a person's sense of security, and that these breach the penumbral privacy rights upon which much of the constitution is premised.

I propose here that those same security rights that were previously violated by the likes of physical searches and quartering may now be violated by pervasive digital searching and tracking in its many forms, or, simply summarized, dataveillance. There is here considerable gap between the constitutional and private law treatment of privacy, and with good reason. Constitutional law is only as wide as the constitution, and the state has only the powers which the constitution grants it—even if there the burden of proof generally lies with the party claiming an action unconstitutional. Private law proceeds from the opposite premise; everything is legal or lawful unless there is a basis for making it illegal or unlawful. The *Griswold* court found that the state (of Connecticut, in that case) had overstepped its powers and encroached on the protected zones of privacy.

One aspect of this question was recently considered in the Supreme Court of the United States in *Clapper v. Amnesty, Inc.*[31] This case was essentially about the standing of the respondents. The state had conducted various data-surveillance programmes, and the respondents—Amnesty International and journalists—claimed their rights were infringed, since they could not communicate freely with certain foreigners since it was, in their view, likely that those foreigners were being surveilled by the US government. This ostensibly caused them expense and inconvenience as they sought various means of secure communications. On this basis, they sought standing to challenge the Foreign Intelligence Surveillance Act (FISA), 1978.

Alito J, for the 5–4 majority, opined:

> Respondents assert that they can establish injury in fact because there is an objectively reasonable likelihood that their communications will be acquired under §1881a at some point in the future. But respondents' theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.' E.g., Whitmore v. Arkansas, 495U. S. 149, 158 (1990).[32]

Amnesty International and others, the respondents, raised two arguments for standing, and each bears consideration in the present context. First, they said that there is 'an objectively reasonable likelihood that their communications will be acquired under §1881a at some point in the future',[33] and this will cause them injury. The court did not deny that this may cause the injury but said instead found that 'respondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.'[34] In other words, there was not sufficient certainty or immediacy of the injury occurring. All were agreed that the injury in question would only occur if there was an objectively reasonable likelihood of respondents' communications being acquired. The court found that there was no demonstrable likelihood.

Second the respondents maintained 'that the risk of surveillance under §1881a is so substantial that they have been forced to take costly and burdensome measures to protect the confidentiality of their international communications; in their view, the costs they have in-

29 *Boyd v United States,* 116 U.S. 616, 630.

30 *Griswold* (n 27), 486.

31 *Clapper v Amnesty International USA* 568 U.S. (2013), no page number is available as of 23 July 2015, but the ruling is available here: <https://supreme.justia.com/cases/federal/us/568/11–1025/> last accessed 23 July 2015.

32 Ibid, second paragraph of Alito J's opinion; page number not available yet.

33 Ibid.

34 Ibid, para. IIIA.

curred constitute present injury that is fairly traceable to §1881a'.[35] The court rejected this claim, basically saying that since their first argument fails—there is no likelihood of their communications being acquired—then expenses they incurred to avoid the surveillance are not injury by the state, but self-incurred. Summarizing the response to both pieces of respondents' argument, the court opined that 'respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending'.[36] The Supreme Court of the United States would not allow standing based on respondents' concern that they may be caught in the surveillance net and calculation that they likely would be. The peculiarities of this case turn on the provisions of the FISA, specifically Targeting Procedures (50U.S. Code § 1881a (i)(2)(B)), but this example can highlight the inadequacy of current surveillance notions in addressing current privacy violations.

In *Clapper*, Breyer J. dissented from the majority opinion, summarizing as follows:

> The plaintiffs' standing depends upon the likelihood that the Government, acting under the authority of 50 U. S. C. §1881a... will harm them by intercepting at least some of their private, foreign, telephone, or e-mail conversations. In my view, this harm is not 'speculative.' Indeed it is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen. This Court has often found the occurrence of similar future events sufficiently certain to support standing. I dissent from the Court's contrary conclusion.[37]

There are, I think, three elements to Breyer J.'s dissent. Each discussed briefly in turn.

One is that Breyer J. seems to believe there is a higher likelihood of respondents' communication being acquired, thus he writes (part III) that 'there is a very high likelihood that Government, acting under the authority of §1881a, will intercept at least some of the communications just described.'[38] So for example if it is agreed that the threshold for standing is a 50% likelihood of respondents' communication being acquired - then the majority thought that respondents had not shown a greater than 49% chance, and the dissent thought they had shown at least a 50% chance.

A second element is that Breyer J. would fix a lower threshold. So for example if the majority required an 80% chance, the dissent made do with say a 50% chance. He shows that case law does not require certainty, and that other cases allow standing based 'reasonable probability' or likelihood (Part IV A). Breyer J. wrote: 'How could the law be otherwise? Suppose that a federal court faced a claim by homeowners that (allegedly) unlawful dam-building practices created a high risk that their homes would be flooded. Would the court deny them standing on the ground that the risk of flood was only 60, rather than 90, percent?'

Third, Breyer J. seems to have a laxer requirement for demonstration of the said likelihood. He will allow 'commonsense inference and ordinary knowledge of human nature' as opposed to the majority which considered the respondents' claims as leaning on a 'highly attenuated chain of possibilities' and essentially undemonstrated. For example, one of the respondents had been a lawyer representing individuals previously investigated in connection with terrorist activities; Breyer J. notes that 'the U. S. government had intercepted some 10,000 telephone calls and 20,000 email communications involving [his client] Al-Hussayen' from which it was, in Breyer J.'s view, reasonably inferred by respondents that their communications would likely be acquired.

Breyer J. thus found several ways to lighten the burden of demonstrating injury and therefore standing for the respondents. Breyer J. does not state a policy position driving this more lenient approach to standing, but it is hinted at in his dissent. He analyses the 2008 amendment to FISA which introduced the statutory provisions in question, writing:

> The addition of §1881a in 2008 changed this prior law in three important ways. First, it eliminated the requirement that the Government describe to the court each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized, basis. §1881a(g). Second, it eliminated the requirement that a target be a 'foreign power or an agent of a foreign power.' Ibid. Third, it diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific privacy-intrusion minimization procedures (though the Government still must use court-approved general minimization procedures). §1881a(e).[39]

Put briefly, §1881a which the respondents sought standing to challenge implemented three notable changes to the law: (i) it allowed mass surveillance, not only targeted, individualized surveillance as before; (ii) it allowed surveillance of citizens and not just foreign powers; (iii) it did away with an important check on the invasion of

35 Ibid, para. IC.

36 Ibid, para. IIIA.

37 Breyer J.'s dissent is available at: <https://supreme.justia.com/cases/federal/us/568/11–1025/dissent4.html> last accessed 24 July 2015.

38 Para. III.

39 Ibid, para. IIA.

privacy that invariably accompanies surveillance. Basically, §1881a brought the law in line with globalized, mass digital communication; Breyer J.'s dissent responds by suggesting a low bar for anticipating injury, and therefore a low bar to standing. He comes very close to saying that if someone is at risk of coming under surveillance, then he should be given standing.

Breyer J.'s dissent must be read against the background of FISA and its purpose, to stop terrorist attacks against Americans. The Hawthorne Effect is a double-edged sword; while lawyers and human rights activists may be prevented from effective communication and may be affected by even the possibility or perception of being a potential surveillance target, so are the terrorists whose removal is the ultimate purpose of the law. The law thus imposes various checks on the cost (the chilling effect on communication, of lawyers and activists) while retaining the maximal benefit (the chilling effect on communications of terrorists); the majority and dissent disagreed on the fulcrum of the cost–benefit analysis of the law, at least with respect to standing, but clearly both sides of the analysis are expressions of the Hawthorne Effect. The debate between the dissent and majority in *Clapper* underscores the need for the law to consider the effects that it has on communication even without direct, immediate, and measurable injury. *Clapper* regarded only the question of standing; but sooner or later, the laws' adaptation to the Information Revolution will lead courts to consider the types of damage that dataveillance inflicts, and they or legislators will find ways to offer protection against such damage.

Information manipulation

The law has long concerned itself with the manner in which one person presents information to the other. Broadly, there has been one-to-many communication which was typically the media—newspapers, books, radio, TV, and websites; and one-to-one/few communication, chiefly personal conversation and correspondence. Alongside freedom of speech and freedom of the press, the law developed tools to protect victims of false communication—defamation in its various modern forms (at least since truth was made a defence), and victims of truthful communication—sedition, blackmail, privacy, and confidence.[40]

Intentional infliction of emotional distress (IIED) was central to a prominent recent case at the Supreme Court of the United States, *Snyder v Phelps*.[41] Snyder's son was a Marine lance-corporal, and was killed in Iraq. The Westboro Baptist Church (WBC) led by Phelps picketed military funerals, vocally and viciously claiming that the death of soldiers, crime victims, and others was on account of toleration of homosexuality in the USA. At the Supreme Court, the majority (8–1) found that WBC was exercising its freedom of speech. Roberts CJ. concluded his opinion thus:

> Speech is powerful. It can stir people to action, move them to tears of both joy and sorrow, and—as it did here—inflict great pain. On the facts before us, we cannot react to that pain by punishing the speaker. As a Nation we have chosen a different course—to protect even hurtful speech on public issues to ensure that we do not stifle public debate. That choice requires that we shield Westboro from tort liability for its picketing in this case.

A lone dissenting voice was that of Alito J.—the same Alito J. as wrote for the majority in *Clapper*—who found that the facts of *Snyder* led to a rare instance of actionable IIED. WBC. . .

> may express their views in terms that are 'uninhibited,' 'vehement,' and 'caustic.' *New York Times Co.* v. *Sullivan*, 376 U. S. 254, 270 (1964). It does not follow, however, that they may intentionally inflict severe emotional injury on private persons at a time of intense emotional sensitivity by launching vicious verbal attacks that make no contribution to public debate. To protect against such injury, 'most if not all jurisdictions' permit recovery in tort for the intentional infliction of emotional distress (or IIED).

This recent case underscores the difficulty in finding actionable IIED. In English law, *Wilkinson* (mentioned by Alito J) first recognized a tort of IIED,[42] but as Lord Hoffman later stated, that case was for causing psychiatric injury, not mere distress.[43] In *Snyder*, the main barrier to actionable IIED was First Amendment Free Speech, and WBC was recognized as exercising its free speech since it was exercising its speech in a public place and on a public issue.

A new form of IIED may need to be legislated or recognized in order to contend with recent innovations in communication—especially social networks à la Facebook, Twitter, etc. One of the novelties of social networks is that they are a platform for one-to-many and many-to-one communications, but in contrast with, say, a newspaper article that a person could formerly write or even an email that they could send to countless addressees, social networks can deliver curated and personalized messages one to many.

40 See Friedman (n 17), p. 9 et seq.

41 *Snyder v Phelps* 562 U.S. (2011).

42 *Wilkinson v Downton* [1897] 2 QB 57.

43 *Wainwright and another (Appellants) v Home Office (Respondents)* [2003] UKHL 53; [2003] 3 WLR 1137.

A recent example of a situation where such a new tort may be needed was provided by Facebook. In June 2014, it became known[44] that data scientists at Facebook tested 'emotional contagion'—basically one person's mood being affected by the moods of those with whom she interacts, the novelty being that they tested it on Facebook. In other words, they examined whether, for example, seeing positive items in one's Facebook feed would result in other being more positive, on Facebook at least, or perhaps the inverse.

> The results show emotional contagion. . . .for people who had positive content reduced in their News Feed, a larger percentage of words in people's status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred. These results suggest that the emotions expressed by friends, via online social networks, influence our own moods, constituting, to our knowledge, the first experimental evidence for massive-scale emotional contagion via social networks. . ., and providing support for previously contested claims that emotions spread via contagion through a network.[45]

Of particular note for our present purposes is not that others can affect our emotion, but that Facebook can. And does. And did, in apparent violation of its own terms and conditions.[46] Facebook used control of the data we received as a means to manipulate the emotional state of users of its service.

In addition to the power that observation can have on who we are, what we do, and how we develop ourselves, the cloud facilitates not only extensive observation but also evaluation. One of the mottos of good teaching and parenting is 'Labeling is disabling'. Put simply, when a parent, teacher, or other person of influence labels a child as 'clever', 'naughty', 'clumsy', and so on, that fixes the child's perception of herself and prevents her from developing her personality.[47] The same is true of each of us. Big Data—collection and analysis of large data sets to reveal various patterns and trends are a corollary and outcome of cloud technologies, and Big Data labels us. Our social lives and social influence are mapped and quantified, our preferences are predetermined, our choices all but made, and our experiences are anticipated. This technological shift endangers our privacy through the influence which financial institutions, information providers, online stores, employers and teachers have over us; influence that was never granted to them but was gained with the emergence of the cloud-enabled technologies. The emerging dangers to our privacy are not in our losing control over data; but in data's gaining control over us.

> The genius of Big Data is that by watching individuals' purchasing, reading, and browsing habits, marketers can identify their personality traits. . .This new research helps explain why American privacy legislators and regulators might resist restrictions on disclosure. . . Because consumption choices reveal personality attributes, the collection of Big Data improves firms' abilities to engage in personality discrimination. . .Maybe the law's tolerance for personality discrimination ought to be questioned, but American antidiscrimination law presently does not regard that kind of question as close.[48]

Discrimination in its many forms and in increasing sophistication is one of the many troubling outcomes of cloud technologies and big data.[49] Once a computer somewhere determines that we are lonely, wealthy, interested in some activity or topic, and so on, we are labelled. Based on our browsing and search, name, zip code, operating system and shopping history, reading interests, social engagement, etc., we 'become' who the web of cloud technologies and platforms tell us we are, and the step from there back into our real world is getting smaller by the day. In other words, our solitude and space for developing our personality are infringed and limited. In Floridi's inimitable words: 'ICTs [information and communication technologies] are re-ontologizing the very nature. . . of the infosphere, and here lies the source of some of the most profound transformations and challenging problems that we will experience in the close future, as far as technology is concerned.'[50] Floridi goes on to say:

> Old ICTs affected the ontological friction in the infosphere mainly by enhancing or augmenting the agents embedded into it; therefore, they tended to decrease the degree of informational privacy possible within the infosphere. On the contrary, new, digital ICTs affect the ontological friction in the infosphere most significantly by re-ontologizing it; therefore not only can they both decrease and protect informational privacy but, most importantly, they can also alter its nature and hence our understanding and appreciation of it.[51]

44 <http://venturebeat.com/2014/06/28/facebook-secretly-experimented-with-the-moods-of-700000-of-its-users/> accessed 19 May 2015.

45 ADI Kramer, JE Guillory, and JT Hancock, 'Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks' (2014) 111 Proc. Natl. Acad. Sci. USA 8788, 8790.

46 <http://www.forbes.com/sites/gregorymcneal/2014/06/30/controversy-over-facebook-emotional-manipulation-study-grows-as-timeline-becomes-more-clear/> accessed 19 May 2015.

47 H Ginnot, *Between Teacher and Child* (Avon Books, NY 1972) 99.

48 LJ Strahilevitz, 'Toward a Positive Theory of Privacy Law' (2013) 126 Harv.L.Rev. 2010, 2023, 2024.

49 See also P Ohm, 'The Underwhelming Benefits of Big Data' (2013) 161 U.Pa.L.Rev. Online 339.

50 L Floridi, *The Ethics of Information* (OUP, Oxford 2013) 6, 7.

51 Ibid, 235.

Translated into English, this means that technology such as cameras, tape recorders, and computers used to reduce our privacy since they improved the flow of information and increased others' potential and actual access to our data. New technological innovation may enhance privacy (eg firewalling, encryption, password protection) or reduce privacy, but either way, new technology actually changes the very significance of our data, or in terms I used above—gives otherwise insignificant and irrelevant data control over us. This is nicely illustrated by the landmark May 2014 ruling by the EU Court of Justice in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos*[52] on the 'right to be forgotten'. In that case, Mr Mario Costeja González lodged a complaint with the Spanish data protection authority against Google, since a search for his name on Google displayed an auction for his house to satisfy a debt to social security. That auction and since-satisfied debt were now 16 years old, and he claimed that under Article 12 of the DPD Google could be required to remove this information. The ECJ agreed and wrote (para. 98) that. . .

> it should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list.

The court's recognition of the right to be forgotten in this case is a recognition that 'labeling is disabling', and that Google's search tool is, in Floridi's terms, a re-ontologizing technology. These old data were given new significance by developments in information technology, in this case Google's search engine. For example, the right, in many jurisdictions, to expunge or seal criminal records was undermined by Internet search engines. In *González*, the data that previously would have sat in a database somewhere in oblivion was presented front and centre to the ongoing detriment of González.

Google is of course not unaware of the significance of what it is doing with old data and the implications for data subjects. Eric Schmidt, chairman of Google, and for over 10 years its CEO, recently said that 'The evolution of Google is to go from you asking Google what to search for, to Google helping you anticipate, to make you smarter'.[53] Google is learning our behaviour, learning to anticipate what we will do so that it can ostensibly help us to do it better, quicker, cheaper, etc. Many will view that prospect as a fine example of data controlling us, with all the implications discussed above.

Social Penetration Theory or a similar metaphor and framework for analysing the multifaceted and multilayered nature of our lives can help to determine which aspects of our lives and personalities need protection, what the source and authority of that protection needs to be, and what its scope. The level of privacy we seek is highly contextual and temporal; we have different bars for privacy at work, at home, or in public. Privacy protection for an individual differs from privacy of corporations, of the deceased, of foetuses, of public figures; it is treated differently for minors and adults and so on. And, these forms of privacy change as technology and society changes. However, they can all be brought within one theoretical framework.

I have shown in this section that existing privacy torts are inadequate to address some of the emerging forms of privacy violation, notably dataveillance and informational manipulation. In the next section, I show how yet another central tenet of privacy law has broken down in the cloud, namely the distinction between horizontal and vertical privacy.

Cloud-enabled technologies merge horizontal and vertical privacy

Long before Warren and Brandeis, the law recognized and protected the privacy of the individual from the state. Different jurisdictions have very different conceptions as to who is the expected villain in the privacy context—third parties, or the state.[54] Thus,

> in the contemporary United States, most citizens understand privacy interests to implicate both nondisclosure and autonomy rights against the government; by way of contrast, privacy law does relatively little to protect citizens against each other or against corporations that seek to collect and sell personal information that arguably fits within the scope of the Warren and Brandeis concerns. In the contemporary European Union, on the other hand, privacy concerns are as much about securing personal information from other private interests, including both other citizens and corporations, as they are about autonomy claims against the government.[55]

This division is getting blurred, but for the most part, it is in privacy as against the state that the impact of the

52 C-131/12, available from <http://curia.europa.eu/juris>, delivered 13 May 2014 [accessed 19 May 2015].

53 <http://money.cnn.com/2014/10/16/technology/innovationnation/google-data/index.html?hpt=hp_bn2> last accessed 19 May 2015.

54 Paul M Schwarz and Karl-Nikolaus Peifer, 'Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept' (2010) 98 CLR 1925, 1927 <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2755&context=facpubs> accessed 19 May 2015.

55 RJ Krotoszynski Jr., 'The Polysemy of Privacy' (2013) 88 Ind.L.J. 881, 883.

cloud-enabled technologies is most acute, for several reasons.

First, the law is much slower to evolve than industry best practices. The law lags technology by years and decades; as Sundquist notes, the US Supreme Court applied Fourth Amendment guarantees to telephony decades after the technology became widely used.[56] There are still more areas in which the law is not yet settled and

> technology untested by law has flourished—examples include respawning cookies, beacons and flash cookies, and browser history sniffing. Governments and businesses build around new, unregulated technology and practices and then claim that changes would endanger their business or national security.[57]

The state, and especially law-enforcement bodies, will tend to act at the cutting edge of the law—taking advantage of the technologies not yet regulated, and interpreting legal provisions to be as permissive as possible of their work. A famous example from the USA is *Kyllo*.[58] Oregon police suspected that Kyllo was growing marijuana, which requires heat lamps. The police involved a federal agency, and the agent, using thermal imaging equipment concluded that there appeared to be heat sources in Kyllo's garage and that Kyllo was growing marijuana. On that basis, police obtained a warrant to search the home, where they then found marijuana. The case eventually reached the Supreme Court. Kyllo claimed that use of the thermal imaging was a search and was subject to his Fourth Amendment rights and required a warrant; police argued that he had no reasonable expectation of privacy in regard to thermal imaging, since he chose not to install thermal insulation that would block the effectiveness of such imaging. The US Supreme Court ruled for Kyllo: the technology was not in common use, and therefore Kyllo had a reasonable expectation of privacy in respect of the thermal signature of his home, and this was then a search within the Fourth Amendment.

In *Kyllo*, US Department of the Interior agent William Elliott first used the Agema Thermovision 210 thermal imager to scan Kyllo's home on 16 January 1992. The Supreme Court gave its decision on 11 June 2001. In other words, it took about a decade for law enforcement to learn conclusively that use of these devices required a warrant. Even then, there were no personal consequences for the agent concerned, and in the intervening years, law enforcement presumably continued with the practice.

Compare that with the Google StreetView case. Between the years 2008 and 2010 Google's StreetView cars laden with multiple cameras drove around taking pictures for StreetView, and also picked up information from and about private Wi-Fi networks. Data Protection Agency (DPA) began investigating in 2010. Google was basically cooperative[59] and apologetic, and did not appeal any of the DPA decisions. In the USA, Google made a multi-state settlement for a $7M fine[60]; in Hamburg, Germany, Google was fined $189,000[61]; and in the UK, Google got off without more than a reprimand, and actions in other jurisdictions are not settled yet.[62] The fines are admittedly small compared with Google's income and cash hoard. However, in addition to the less than negligible fines, Google's reputation has incurred a cost from the violations, and contending with these many investigations—even cooperatively—carries a considerable expense, probably amounting to more than the fines.[63]

Facebook's Beacon service that notified a user's friends of various online transactions that a user may make caused an uproar for its trampling users' privacy. The service quickly fomented a class action, which Facebook settled for a $9.5M settlement fund, in addition to approximately $3M in the claimants' attorney's fees.[64] Presumably, the true direct and indirect costs were considerably greater than that both in legal expenses and in reputational damage.

Both the Google StreetView and Facebook Beacon examples, as compared with *Kyllo* and such cases, suggest that enforcement may be considerably more effective against companies than against the state. This difference is for the most part well justified by the values served by the state. Agent Elliott tried to stop marijuana from hitting the streets, whereas corporations are profit maximizers, even if they ostensibly seek to make the world a better place at the same time. Unsurprisingly,

56 M Sundquist, 'Online Privacy Protection: Protecting Privacy, the Social Contract, and the Rule of Law in the Virtual World' (2012) 25 Regent Univ.L.Rev. 153, 164.

57 Ibid, 162.

58 *Kyllo v United States* 533 U.S. 27 (2001) 190.

59 Google was fined for delaying a Federal Communications Commission investigation: <http://www.wired.com/images_blogs/threatlevel/2012/05/unredactedfccgoog.pdf> accessed 19 May 2015.

60 <http://www.ct.gov/ag/cwp/view.asp?Q=520518&A=2341> accessed 19 May 2015.

61 <http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease_2013-04-22_Google-Wifi-Scanning.pdf> accessed 19 May 2015.

62 <http://www.wired.co.uk/news/archive/2013-06/21/google-data-street-view> accessed 19 May 2015.

63 More recently still, Google was fined $1.2M by Spain's DPA <http://www.bloomberg.com/news/2013-12-19/google-fined-1-2-million-by-spain-s-privacy-watchdog.html> [accessed 19 May 2015] for other violations.

64 <http://www.reuters.com/article/2013/11/04/us-usa-court-facebook-idUSBRE9A30LM20131104> accessed 19 May 2015.

people and companies are punished by markets, courts, and regulators with much greater immediacy and efficacy than the state is, and in cases such as StreetView and Beacon, the damage to the brand greatly outweighs any regulatory or judicial punishment, which explains why Google and Facebook were quick to cooperate. The state is much more inclined to attempt privacy brinksmanship and even reckless or intentional violations of privacy law than corporations are. Were it not for the indiscretions of Edward Snowden, the massive invasions of privacy undertaken in PRISM, Tempora, and other enormous state programmes would not even have come to the public's knowledge, and it still remains to be seen what will change now that the public is aware of them.

Second, the state's many bodies can and do share information and collaborate both on data collection and on analysis, with the result that dangers to privacy are compounded in the public sector. In Israeli law, Section 23B prohibits the state from handing over personal data from its database, unless the data subject consents, but Section 23C provides that such data may be transferred from one public body to another unless prohibited by some other legislative provision.[65] In *The Association for Civil Rights in Israel v Ministry of Interior* ('*ACRI*'), the Israeli Supreme Court had to rule on whether the Israeli Ministry of Interior could allow other state bodies—specifically the Income Tax Authority, the National Insurance Institute of Israel (ie Social Security), and the Israel Broadcasting Authority, and banks that needed to verify the identities of clients—direct access to the Ministry's citizen database that included such information as age, date of birth, address, and children. Dorner J. wrote:

> The wise easily understand[66] that the practice described in the State's and the banks' responses falls short in the 'minimal harm' test. For the transfer of data to public bodies is not limited only to those employees who need the data for their work. Even efforts undertaken to ensure that the data will reach only those public-sector employees who need it cannot substitute provisions in regulations or, at the very least, administrative guidelines. The proportionality-requirement necessitates mitigating the violation of the right to privacy by limiting the number of public-sector employees with access to the data, by limiting the scope of the data transferred, such that only data that is required is transferred; and by considering the importance of the purpose for which the data is required when establishing the scope of the data [to be transferred].[67]

Gronis J. took a different view. Banks are required by Israeli law to demand a national ID card from someone opening an account. They are also required to verify the information presented to them with the Ministry of Interior, and the data they receive are the same as the data presented in the card. There is effectively, therefore, no additional invasion of privacy flowing from the data transfer, and if there is, it is *de minimis*. And anyway, adds Gronis J., these are hardly as personal as the data which a bank clerk already has on the person—such as detailed financial information.[68] But as Gronis J. specifically wrote,[69] the outcome of his analysis described above was that the transfers to the banks ought to be allowed; as regards transfers to the public bodies he endorsed the view of Dorner J. The Supreme Court was thus split as to the harm that came from allowing banks access to a state-owned database of citizens' national ID data; but the court was unanimous that allowing state institutions, such as the Income Tax Authority, access to the national ID database had to be severely curtailed; specifically that only information required could be given, and that data had to be requested specifically for each individual citizen.

This case was brought as a 'High Court of Justice' case, meaning that it involved judicial review of state decisions. The many victims of the apparent invasions of privacy got no compensation or redress—the case was brought by a civil rights society, and it was decided 6 years or so after first being filed. In other words, this case was but one instance of state violation of data protection provisions, and the case was brought by an non-governmental agency and offered no comfort to individuals already harmed. In addition to the harm resulting from the state institutions' unfettered access to the database, the wholesale access afforded opportunities for specific abuse. Indeed, the petitioner submitted in support of its case an indictment of 50 civil servants who had transferred personal information accessed from government databases to private detectives.[70] The court's unanimous imposition of stringent restrictions on transfer of data between state institutions, contrasted with the split opinions as to transfer from the state institutions to the banks, gives the impression that it viewed the state's violations of privacy as rather more sinister.

The agreement between Dorner J. and Gronis J. underscores the growing concern in Israel with abuses of privacy by state institutions. Increasing use of the cloud storage and applications providing a massive

65 See discussion in SCJ 7256/95 *Pinhas Feischler v Chief of Police* PD 50(5)1.

66 A phrase borrowed from Proverbs 14:6.

67 SCJ 8070/98 *The Association for Civil Rights in Israel (ACRI) v Ministry of Interior* PD 58(4) 842 at 852, para. [7] per Dorner J., my translation.

68 Ibid, 862, para. [9] per Gronis J., my translation.

69 Ibid, 857 and 858, para. [3].

70 Ibid, 849, para. [4] per Dorner J.

pool of data, along with the reduced effectiveness of traditional wiretaps, means that government surveillance is increasing.[71] It is becoming considerably easier for the state to dramatically increase surveillance, including wholly unjustified and unnecessary data collection of citizens. For example, as more and more aspects of citizens' lives go online, everything from their financial information and health records to their political affiliations and relationships are either stored in the cloud or are easily determined from analysing data in the cloud. Though enforcement against the state is likely to be much slower and less effective than enforcement against private-sector persons, the potential for abuse by the state and the scope of the resulting harm is considerably more worrying, and surveillance by the state using the cloud-enabled technologies significantly increases both the ease and the impact of abuse. This was evident when Edward Snowden brought to light the extent of government agency use of private-sector enterprises for surveillance.

Third, the state has resources that can be used for privacy-invasive practices and that are available to very few individuals or corporations. An early and famous exception was Walmart, which in the 1980s created its own satellite network and used it for everything from inventory management (ostensibly its main purpose), to training, increasing the speed of credit card payment processing, and even broadcasting a concert live to its stores. Nowadays, Google, Apple, and Samsung might be seen as exceptions to this rule. Still, major privacy-invading systems à la PRISM and Tempora with their enormous telecom metadata gathering through corporations and Upstream which had the National Security Agency hacking the internet backbone, as well as using satellites and drones, extensive wiretaps and surveillance, and more are beyond the reach and culture of even these massive corporations.

Yet all this may be changing. There is a long history going back almost four decades of investigation of CIA use of satellite surveillance in the domestic USA.[72] In the meantime, publically traded multi-billion-dollar market capitalization companies such as Digital Globe can provide high-resolution satellite imagery of anything to anyone, for a price. Google has gone a step further and recently acquired its own satellite capabilities with the 2014 acquisition of Skybox Imaging, a 5-year-old company that builds and launches its own satellites and uses them for massive image collection and processing.[73] The same goes for drones. Following recent revelations that the FBI has been using drones within the USA,[74] some states rushed to pass legislation restricting law-enforcement use of drones. For example, the Florida senate promptly and unanimously approved the Freedom from Unwarranted Surveillance Act, but that act restricts law-enforcement use of drones, leaving, for now, open skies for civilian use. It will not be long before companies like Digital Globe sell drone data and imagery to all buyers, law-enforcement included. Amazon, Inc.'s recent announcement that it will use drones for delivery raises the prospect of hordes of octocopters flying all over the city making deliveries; using them simultaneously for data collection is an obvious utilization of that resource. Rapid technological change in satellites, drones, cloud computing, wearable computing, and more will continue to afford opportunities to try out new privacy-invading technologies until courts and consumers catch up. As Oppenheimer notes:

> Running throughout this evolution is the common thread of protection of privacy and dignity interests against arbitrary and invasive acts by the government. However, the meaning of 'invasive' has historically evolved in response to technological advances, and technological changes have been dramatic since the Supreme Court's most recent venture into Fourth Amendment theory.[75]

The state will also test new privacy-invading technologies and techniques, while the courts take their time examining their legal status. More importantly, for privacy, the lines between industry and government are getting blurred in the use of cloud-enabled technologies, and other cutting-edge technologies discussed above, such as drones, wearable computing, and commercial satellites.[76] The Supreme Court of the United States has held that Fourth Amendment privacy rights vis-à-vis the state do not apply to data transferred to a third party, the 'third party test': 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'[77] This was mostly reasonable in a world in which people generally held onto their own data,

71 P Swire, 'From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek access to the Cloud' (2012) 2 IDPL 200.

72 For a thorough history of satellites and US law, particularly with an emphasis, see RA Best Jr. and JK Elsea 'Satellite Surveillance: Domestic Issues' (2011) Congressional Research Services <http://www.fas.org/sgp/crs/intel/RL34421.pdf> accessed 19 May 2015. See also: P Korody, 'Satellite Surveillance Within U.S. Borders' (2004) 65 Ohio St. L.J. 1627.

73 <http://www.forbes.com/sites/ellenhuet/2014/06/10/google-buys-skybox-imaging-not-just-for-its-satellites/> accessed 19 May 2015.

74 See the US Department of Justice report: <http://www.justice.gov/oig/reports/2013/a1337.pdf> accessed 19 May 2015.

75 MS Oppenheimer, 'Cybertrash' (2011) 90 Or.L.Rev. 1, 4.

76 Along similar lines see Krotoszynski Jr. (n 44), 893, citing OM Fiss.

77 *Smith v Maryland*, 442 U.S. 735, 743 and 744 (1979). See discussion in AW Bagley, 'Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects' (2011) 21 Alb.L.J.Sci.& Tech. 153, 174.

storing them in their own local files and computers. However, as noted by Bagley, this doctrine is a very poor match for the reality of consumer cloud computing.

> The Internet is run primarily by private entities beginning with the cable, telephone wire, or wireless network running into a user's home all the way to the webpage on a remote server accessed by their computer. Therefore, users interact with a myriad of digital third parties in every online activity from sending an email to navigating the Web. As such, users' expectations of privacy appear inconsistent with traditional notions of third-party 'false friends' when applied to online communications.[78]

This is true a fortiori for widely used technologies such as iCloud, Google Drive, Dropbox, and Amazon Web Services, which have droves of consumers and businesses regularly storing and using data at and through service providers. In this way, privacy vis-à-vis the State and privacy vis-à-vis third parties blend in the cloud, and the coming years will likely see significant changes in the way the law treats the flow of private information from an individual, to a third party, to the state. This brings us to an additional important point, made by Krotozynski, particularly relevant in considering Israeli privacy law. He notes that whereas, in the USA, 'privacy' is generally associated with protection from state intrusion in our data, in Europe, and specifically in Germany, data protection and privacy are considered parts of the greater value not of 'privacy' but of higher and more general values such as 'human dignity' and 'development of the personality'. Krotozynski demonstrates that the German prohibition on Holocaust denial is a further instance of a general protection afforded to 'human dignity' and contrasts this with the American Constitution's passionate protection of Freedom of Speech. This, along with privacy, is another example of the German (and more generally European) model of privacy as an expression and protection of human dignity, as opposed to American privacy as a right that keeps the state at arm's length. Whether or not Krotozynski is right about this comparison of privacy in the USA and Germany, in Israel at the Supreme Court, Gronis J. in *ACRI* specifically recognized that privacy from others and from the state are two sides of the very same constitutional coin:

> There are two aspects to the right to privacy mentioned in section 7(a) of the Basic Law: Human Dignity and Liberty. One aspect, the sources of which may be found in human dignity, is that 'a person has a right to manage his lifestyle in the four cubits[79] of his home without outside interference.' This statement is not to be limited to the physical facet of his home. It is to be understood more broadly construed, metaphorically, in the spirit of the phrase coined by Warren and Brandeis: 'the right to be left [sic] alone'. The other aspect deals with fear of the state's excessive power, that it will concentrate too much information regarding citizens and residents and will make wrongful use of that information.[80]

Gronis J.'s dictum here reflects the two strands identified by Krotozynski as American and European and brings both within the rubric of 'human dignity', as do later cases.

Tene has argued cogently that the Israeli law of privacy initially reflected the American model and morphed into the European model following the passage of the Basic Law.[81] There are grounds for the position that this shift has not quite taken place.[82] Indeed, before the Privacy Law was even passed or its provisions finalized, then Minister of Justice Tamir specifically referenced the draft of what would later become the Basic Law to make the point that protection of privacy will soon be the subject of constitutional protection.[83] But, nevertheless, it is agreed that in the post-Basic Law reality, Israeli law today is close to the European tradition of privacy law. The Israeli Supreme Court has expressly determined that the Basic Law must guide the interpretation of all parts of the Privacy Law; in other words, the collection and use of data under Chapter 2 of the Privacy Law were to be interpreted under the influence of Section 7 of the Basic Law.[84] In other words, both Chapter 1 privacy and Chapter 2 data protection are expressions of 'human dignity and liberty' under Israeli law.[85]

In this way, Israeli law has already prepared the ground for bringing the privacy protection of individuals, data protection regulation, and the constitutional protection of privacy all under one legal umbrella. That transition is likely to accelerate as cloud-enabled

78 Bagley, ibid, 174 and 175. See at length also JL Simmons, 'Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People"' (2009) 3 Colum.Bus.L.Rev. 950.

79 This is a concept drawn from Jewish law—namely the four cubits (approximately 2 m) around a person are treated as his personal space in law, lore, and literature.

80 ACRI (n 56), 856, para. [2]. Gronis J. wrote a minority opinion, but this point was not in dispute.

81 O Tene, 'The Right to Privacy following the Basic Law: Human Dignity and Liberty: A Conceptual, Constitutional, and Regulatory Revolution' (2009) (Heb.) 8 Kiryat Mishpat 39.

82 A Schreiber 'Jewish Law Privacy – A Historical and Conceptual Analysis' (2013) 20 JLA 179, 227.

83 Rashumot 1453, p. 3487, 23 June 1980.

84 ACRI (n 56), 853. This in itself is unexceptional. The Supreme Court of the United States had held in *Whalen v. Roe* 492 U.S. 589 (1977) that the Constitution protects information privacy. See discussion in Strahilevitz (n 37) 2015 et seq.

85 See discussion in Tene (n 70).

technologies, and other technological developments continue to spread wider and deeper into the fabric of daily life.

Conclusion

Cloud-enabled technologies are changing the ways in which privacy is challenged in three important ways.

First, though many have emphasized privacy as control of information, when considering cloud-enabled technologies, it is privacy as protecting the sense of self that is most immediately challenged.

Second, recently emerged technologies enable new forms of damage to victims of privacy violation. Two in particular were examined, namely dataveillance and information manipulation. New forms of tort may be required to adequately protect against these forms of damage.

Third, one of the most important distinctions in privacy law—that between horizontal and vertical privacy—is breaking down. The law needs to formulate a more general, holistic approach to privacy that will treat both sides of privacy, particularly at the points of intersection and overlap.

doi:10.1093/idpl/ipv015