The Role of Privacy in a Changing World

Chris Boam[*]

In October 2013, I was interviewed for an article that appeared in the Christian Science Monitor.[1] The topic was the U.S. NSA surveillance revelations and their potential impact on U.S.-European Union trade and other key negotiations. A friend, someone who had been forwarded a copy of my remarks, emailed me with the following kernel of resignation: "our privacies once enjoyed are a thing of the past."

I have heard variations on this theme for many years, even more of course within the past year. In May 2013, Judge Richard Posner of the Second Circuit wrote an editorial for the New York Daily News calling privacy "overrated."[2] His core theme – that privacy and security are in constant balance against one another – is very sound, even if his enthusiasm for security to be ever favored in the balance might today be seen as understandable pre-NSA revelations exuberance. An August 12, 2013 article in Time magazine, highlighting that privacy is "illusory"[3] just days after the NSA audit reports on privacy violations were made public, was less excusable. It reminded me of an old Monty Python sketch – the British policeman standing in the midst of a melee, holding a bull horn and calmly imploring, "Please disperse, there is nothing to see here."

In late November 2013 at the U.S. Federal Trade Commission's (FTC's) forum on the "Internet of things," a long-awaited discussion of the swirl of issues brought about by the

---

* 40A&M LLC, Northern Virginia, USA.

1. *See generally* Clayton, Mark, "U.S. Spying in Europe: will it backfire on Google and Facebook," Christian Science Monitor (Oct. 24, 2013), at: www.csmonitor.com/World/Security-Watch/2013/1024/US-spying-in-Europe-Will-it-backfire-on-Google-and-Facebook.

2. *See* Posner, Richard A., "Privacy is Overrated," NY Daily News (Apr. 28, 2013), at: www.nydailynews.com/opinion/privacy-overrated-article-1.1328656.

3. *See* Von Drehle, David, "The Surveillance Society," Time (Aug. 1, 2013), at: nation.time.com/2013/08/01/the-surveillance-society/.

prospect of connecting everyday devices, cars, power, etc. to the Internet, Vint Cerf remarked that "privacy may actually be an anomaly," if not a product of our modern industrial age.[4] He described a time when people lived in small villages, and everyone knew everyone else's business. When we began moving into cities, he argued, we developed anonymity as a by-product of urbanization.

What is privacy and why is the view of privacy's lessening relevance in the information age simply not credible? Let us start first by debunking the notion that privacy is of a modern origin. Regardless of whether you are Christian, it probably would not surprise you to learn that the authors of the book of Genesis, in the first-to-second century AD, were interpreting already age-old stories and legends passed down for generations earlier. Thus, it is also likely not surprising that when Adam and Eve in Genesis 3:8-9 are suddenly aware of their nakedness and reach for leaves to construct a bit of privacy, the authors make no reference to an "app for that".

1. PRIVACY IS NEBULOUS, BUT ITS FUNCTION IN SOCIETY IS NOT

On Tuesday, December 4, 2013, the White House's Nicole Wong, Deputy Chief Technology Officer made – for her – a rare set of remarks at a "practical privacy" meeting of the International Association of Privacy Professionals (IAPP) in Washington. In her remarks, Ms. Wong cited the late privacy scholar Alan Westin's premise, that privacy itself is not an "end state" but that the end state is freedom of expression, with privacy as a "means" to that end.[5] This reference to Westin's seminal writings is spot-on, but there is much more to what he said.

---

4. *See,* e.g., Forbes, "Do smart devices need regulation? FTC examines Internet of things," (Nov. 23, 2013), at: www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/.

5. *See* Bracy, Jedidiah, "White House's Wong Makes the Case for Embedded Privacy Pros," IAPP Privacy Advisor (Dec. 4, 2013), at: www.privacyassociation.org/publications/white_houses_wong_makes_speaking_debut_at_iapp_event.

Westin was speaking here to one of three facets to privacy[6] – "informational" privacy. The second facet for Westin, "territorial" privacy, refers to the ability to control the information that enters and leaves our personal sphere. And finally, privacy "of the person" describes a person's right to be protected against undue interference of a physical nature (e.g., why issues of birth control, abortion and commitment proceedings are typically framed as privacy issues). Privacy of the person is so closely grounded – often controversially – by state and federal statutes and case law, that it is best addressed on its own.

Westin wrote that informational privacy is "the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others."[7] Freedom of expression, though critical and particularly in the context of the U.S. Bill of Rights, is only one part of the equation. To use an analogy, Adam and Eve – when they decided to cover their nether regions with leaves – were not likely doing so with the aim of making a statement but rather of not making one. To say nothing, and not have that "nothing" by itself interpreted as expression, is just as vital, but this form of protection requires communal action or standards to blunt whatever interpretive value might be drawn from daily lives.

To use Vint Cerf's example (but in a way, turn it on its head), when a late Victorian tight knit Italian or Jewish community in New York City may have decided to "look the other way" when the local priest or rabbi would regularly imbibe too much on a Friday night, they were creating privacy by social construct. When various cultures and ethnic

---

6. *See,* e.g.*,* Westin, Alan F., "Privacy and Freedom," 25 Wash. & Lee L. Rev. 166 (1968); Westin, Alan F., "The Political and Social Dimensions of Privacy," Journal of Social Issues, Vol. 59, No. 2 (2003), at: www.privacysummersymposium.com/reading/westin.pdf; Bracey, Jedidiah, "Westin's Privacy Scholarship, Research Influenced a Generation," IAPP Privacy Advisor (Mar. 1, 2013), at: www.privacyassociation.org/publications/2013_02_19_westins_privacy_scholarship_research_influenced_a_generation.

7. *See ibid.*

groups urbanized, privacy was hardly thrown to the wind. It was often even more fervently guarded as a critical maintenance of culture. Similarly, when any set of neighbors lives in close proximity long enough, watch programs develop, block parties can happen, but also, the occasional harmless indiscretion of a neighbor child's tantrum is winked at. This is society creating a sense of dignity – the state or quality of being worthy of respect. This is human. Privacy is dignity.

For so much of early U.S. history, the maintenance of privacy as a bulwark of dignity was very much driven by our religious and ethnic socialization. The social standards of what was private were embedded in immigrant traditions – from Western and Eastern Europe, Africa, Asia and then Central and South America. These traditions were carried like a comfortable blanket from home into growing communities of like-minded and like-empowered homogenous people. Even in the close confines of East Harlem, proximity did not blot out privacy. To the contrary, a sense of dignity required it.

As these communities dispersed, the maintenance of dignity through privacy became rooted in far more practical concerns. Even today, as Rosa Brooks wrote so well in Foreign Affairs in late 2013, we are most often concerned with very concrete kinds of economic and physical harm – from social stigma, to job loss, to theft, injury, imprisonment, death[8] – and not an often nebulous vision of what is or is not private. Privacy, in the context of these concerns, supports dignity as a defense against the harms that can flow from power, its uses and abuses. We fear that we'll end up on a "no-fly" list, or be unable to get a security clearance, a job or a loan.[9] From a neighbor using our past as leverage, to a thief knowing where we keep our jewelry, to a government seeking to curtail dissent or worse – what frightens us most is the very concrete possibility that information about us, however it is gleaned, will be misconstrued, misused or abused.[10]

---

8. Brooks, Rosa, "Privacy is a Red Herring," Foreign Affairs (Nov. 7, 2013), at: www.foreignpolicy.com/articles/2013/11/07/privacy_red_herring_debate_NSA_surveillance_debate.

9. *See ibid*.

10. *See ibid*. Recognizing that, even as we debate the issues here, Courts may already be adjusting their views on when or if it is necessary to show "harm", as the Eleventh

Individuals began to look more often to the law for the maintenance of dignity through privacy. Indeed, the greatest growth in U.S. case law on issues of privacy occurred in the periods following late 1800s industrialization and post-World War II, times of great movement, resettlement and technological development in the U.S. The Internet and advance of the information age – while welcomed for all it can do for economic growth, education and global communications – has only exacerbated the gap between our concrete fears regarding data misuse and the maintenance of dignity through privacy that had once been the domain of cultural and religious traditions.

2. HAS LAW BRIDGED THE GAP – ASSUMING THAT WE KNOW WHAT THE "GAP" IS?

Omer Tene, Vice-President of Research and Education to the IAPP, wrote a fascinating blog in March 2014 on the comparison between European and U.S. privacy regimes.[11] His primary point was that, where the U.S. regime may be lacking in depth and omnibus-type issue coverage, tremendous growth in the practical abilities of privacy professionals have made the U.S. address of privacy issues far more activist and effective.

What the U.S. privacy practice has learned particularly well in the past five years is to exploit trigger words underlying privacy-related concerns: secrecy, hypocrisy, deception,

---

Circuit did in remanding negligence and breach of contract, among other claims, in the *Avmed* case, prompting an eventual settlement without a show of harm. *See* Vijayin, Jaikumar, "Court Approves first-of-its-kind Data Breach Settlement," ComputerWorld (Mar. 12, 2014), at: www.computerworld.com/s/article/9247017/Court_approves_first_of_its_kind_data_breach_settlement.

11. *See* Tene, Omer, "The U.S.-EU Privacy Debate: Conventional Wisdom is Wrong," for IAPP (Mar. 4, 2014), at: www.privacyassociation.org/privacy_perspectives/post/the_u.s._eu_privacy_debate_conventional_wisdom_is_wrong.

unfairness.[12] While the public and press may not really understand what "privacy" is – a lack of understanding that many have used effectively to advocate inaction – these individual pulses within privacy are readily relatable. This activism and practitioner abilities are admirable. It is why we are today having this conversation. But, to continually throw incredibly competent soldiers into the breach will not, in this case, cure the breach.

It is impossible, of course, to possess total privacy. Neighbors can peek through our windows, strangers in public places or waiting rooms may see us in the context of what some call the "fine art" of people watching, patrons in cafés can listen in on our conversations and telephone calls, anyone can Google us – and these examples are nothing compared to the data compiled about us by marketers and data brokers. For the most part, this does not trouble us and we simply accept it as the price of living among humanity in an information age.[13]

And yet, it is one thing to know that anyone can see into your kitchen through the window, but another thing altogether to discover someone staring fixedly at you.[14] This triggers not only Westin's notion of "territorial privacy," or the ability to control the information that enters and leaves our personal sphere, but also brings applicable harms to the fore. The man staring fixedly through our kitchen window bothers us not because we think he might discover us doing something "secret," but because he has violated forms of socially acceptable behavior in a way that not only makes him unpredictable,[15] but also, will likely cow our own behaviors in what we thought was a safe environment. "Peeping Tom" laws have been created to address such fears. And similarly, statutes and case law have developed to prohibit the observation of us without our consent in private

---

12. Carson, Angelique, "Changing Tactics: the Rise of the Privacy Advocates," IAPP Privacy Advisor (Sept. 23, 2013), at: www.privacyassociation.org/publications/changing_tactics_the_rise_of_the_privacy_advocates.

13. *See* Brooks, *supra* note 8.

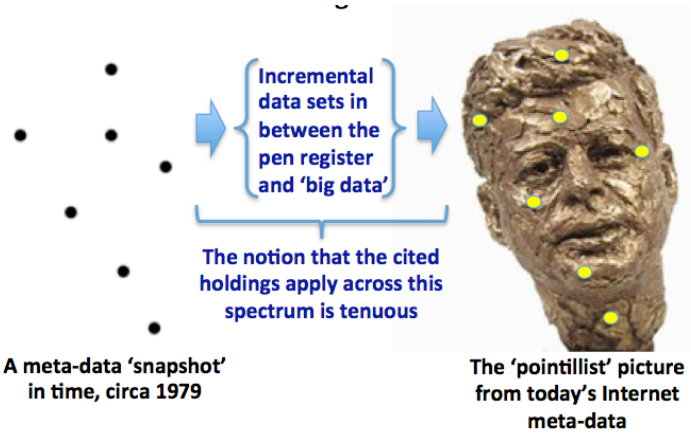
14. *See ibid.*

15. *See ibid.*

spaces or in our homes, by strangers, spouses or significant others. His violation of these norms of acceptable behavior begs the question – will the person be a blackmailer, a thief, a rapist or a murderer, or will the actions merely represent an unacceptable lapse in judgment? Regardless of how these questions play out, the impacts are very real.

At what point does our data profile and how it may be used reach the point where it equates to the man staring fixedly at us through the window, albeit the window of our laptop? The data can be as innocuous as the empty header to an email containing the message "happy Friday," or as fleeting as a time-stamp indicating when we last visited Amazon.com. But combine many thousands of these data points – often referred to as meta-data – with knowledge of who we are, where we live, our buying habits. Add in other types of media content, such as pictures, digital recordings and video. At some point in the combination process, and it may in fact be very early, a picture begins to form – one that is far more "territorial" than merely "informational" in Westin's sense. In October 2013, I gave a presentation where I used the following graphic. It was developed to illustrate the concepts at-issue in applying the 1979 Supreme Court precedent in *U.S. v. Maryland*[16] to today's information environment, but it is useful for larger purposes here.

Figure 18.1



Data brokers, for instance, are increasingly aggregating data about us from numerous sources into ever more specialized lists. The lists, which are typically sold to marketers, presume to cover very sensitive topics regarding the data targets, including: "gay and lesbian adults"; "people suffering from bipolar disorder"; "people with alcohol, sexual

16. 442 U.S. 735 (1979).

and gambling addictions"; and "people who have purchased adult material and sex toys."[17] Currently, data brokers are required by federal law in the U.S. to maintain the privacy of a consumer's data only if it is used for credit, employment, insurance or housing. Medical records and prescription purchases are off limits, but data brokers are allowed to track purchases of over-the-counter drugs and other related medical items to gather a health profile of the data subject.

Even if we are to consider the more restrictive route of requiring consent from a data subject, as in the context of the EU data protection directive, there remains the problem highlighted by Marc Rotenberg. "How do you consent to the disclosure of your information if you don't know which of your information will be disclosed, to whom and for what purpose?"[18] This last question – for what purpose? – is a big one. Even if we are to set aside for a moment the fact that the highly sensitive data in many of these lists is itself an issue, the conclusions drawn by the list makers may bear little resemblance to reality. Just because a metric is easy to capture does not mean it is the right one to use.

Ken Cukier and Viktor Mayer-Schoenberger write in their most recent book, "Big Data – A Revolution", that "causality is nice when you can get it," but the "problem is that it's often hard to get, and even when we think we've found it, we're often deluding ourselves."[19] Seeing "causality" where it truly does not exist in any real or even slightly credible form is the real downside of an over-reliance on "big data" analytics alone. For instance, there is an increasing value in "data exhaust", or the data that is shed as a by-product of action or inaction. However, most individuals that see the value in measuring a

---

17. *See* Roberts, Jeff John, "With Data Brokers Selling Lists of Alcoholics to Big Business, the Feds have some Thinking to Do," Gigaom.com (Mar. 13, 2014), at: gigaom.com/2014/03/13/with-data-brokers-selling-lists-of-alcoholics-to-big-business-the-feds-have-some-thinking-to-do/.

18. *See* Declan McCullagh, Senators Prepare to Vote on Netflix and Email Privacy, CNet (Sept. 20, 2012), at: news.cnet.com/8301-13578_3-57516501-38/senators-prepare-to-vote-on-netflix-and-e-mail-privacy/.

19. Cukier, Kenneth and Mayer-Schoenberger, Viktor, Big Data: a Revolution that will Transform how we Live, Work and Think (Harcourt 2013), at 191.

"negative" – i.e., I did not press X or "opt out" – would tell you that to assign any direct meaning to the inaction is almost never correct.[20]

As Daniel Solove wrote in a terrific article in January 2014 entitled "10 Reasons Why Privacy Matters," even in the off-line world, "knowing private details about people's lives doesn't necessarily lead to more accurate judgment about people. People judge badly, they judge in haste, they judge out of context, they judge without hearing the whole story, and they judge with hypocrisy."[21] Cukier and Schoenberger caution that big data is likely to provide the temptation to judge on the basis of propensity – a temptation that society must be careful to squelch.[22] This is particularly true if the propensity-based decision-making at issue influences choices or options of the data subject, or worse, impacts their reputation, health or livelihood.

This is *not* to say that the data portrait we might have of us, our lives and behaviors cannot be incredibly rewarding. As I wrote in September 2013, companies must keep their focus on the customer and customer choice. If they do this, I believe there is little fear in the short term that a loss of trust among certain national actors will somehow translate to the consumer and damage confidence in consensual services and digital innovations. And if the company is a step removed from the customer, as in the case of many data brokers, something needs to come into play to facilitate that trust. In my podcasts in late July and early August of 2013,[23] I spoke of the many companies – in the "big data" analytics space, for example – that are doing their ablest to find the sweet spot between "killer app" and "creepy app." Much of this effort is growing in the context of

---

20. *See ibid*. at 113-115.

21. Solove, Daniel J., "10 Reasons Why Privacy Matters," a LinkedIn Influencer blog (Jan. 13, 2014), at: www.linkedin.com/today/post/article/20140113044954-2259773-10-reasons-why-privacy-matters.

22. *See* Cukier, *supra* note 19, at 151.

23. *See* 40A&M in 5, at: www.40a-m.com/40am-in-5.html.

predictive search, advertising and applications (the New York Times[24] and Forbes[25] have each done excellent pieces on this). Anticipatory computing and other artificial intelligence – systems that learn to predict what you need before you ask[26] – may not be for everyone, but they will be (and in a limited sense, already are) for some of us.

There is no doubt, as European Commission Vice-President Neelie Kroes said in March 2014, that "the next phase of the Internet will be data centered and connectivity driven. Cloud computing, big data, the Internet of things; tools which support manufacturing, education, energy, our cars and more."[27] However, "to make the leap of faith into this new world," as she put it, "reliability and trust is a pre-condition."[28] In the absence of law that establishes when data collection equates to "staring fixedly at us" through our computer, or at the very least recognizes and protects highly sensitive categories of data, erosion in the economics of trust (EOT)[29] will become an ever more

---

24. *See* Miller, Claire Cain, "Apps that know what You Want, Before You Do," New York Times (Jul. 29, 2013), at: www.nytimes.com/2013/07/30/technology/apps-that-know-what-you-want-before-you-do.html?pagewanted=all&_r=2&.

25. *See* Hill, Kashmir, "How Target Figured out that a Girl was Pregnant Before Her Father Did," Forbes Tech (Feb. 16, 2012), at: www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

26. *See* Hu, Elise, "Computers that know What You Need, Before You Ask," NPR All Things Considered (Mar. 17, 2014), at: www.npr.org/blogs/alltechconsidered/2014/03/17/290125070/computers-that-know-what-you-need-before-you-ask.

27. Kroes, Neelie, Vice-President of the European Commission responsible for the Digital Agenda, "Securing our Digital Economy," CEBIT Cyber-security Conference (Mar. 10, 2014), at: europa.eu/rapid/press-release_SPEECH-14-197_en.htm.

28. *See ibid*.

29. The EOT is a concept that I first introduced in "Privacy in Transition: the U.S. and EU Strive for Meaningful Change in the Midst of Emerging 'Economics of Trust,'" (Jan.

measurable reality. Erosion in the EOT is best represented as the moment when a lack of comfort, either in transparency or follow-through by an industry or government translates to accelerating decisions by a consumer not to press "send," "purchase," or "I agree."

3. THE SEA CHANGE IN THE ROLE OF TRUST

When I wrote in January 2013[30] that the EU-U.S. privacy relationship had several fundamental stumbling blocks, despite many mutual goals, I did not expect that "investigative measures" would be the one stumbling block to soon dominate the news. From the first notices from former NSA contractor Edward Snowden of a bulk telephone meta-data database, to most recent revelations (as I am writing) of "Mystic," the bulk collection of an entire country's recorded telephone conversations,[31] the breadth of surreptitiously collected information – most of it swept up and warehoused without a trigger of investigative purpose – is staggering.

For a time after June 5th, I tried to see things from the perspective of some in Congress who, despite the waves of revelations, seemed conflicted with regard to what should be done. We do not see the oppression of a virtual invasion of privacy very much, and "you cannot hold up a picture of someone being electronically spied on."[32] Even worse, you cannot immediately illustrate the "psychic damage and cowed sensibilities that come with

---

23, 2013) 40A&M and Intermedia, at: www.40a-m.com/uploads/3/1/9/0/3190984/privacy_in_transition_full_article_23_jan_13.pdf.

30. *See ibid*.

31. *See* Gellman, Barton and Soltani, Ashkan, "NSA Program Reaches into the Past to Retrieve, Replay Phone Calls," Washington Post (Mar. 18, 2013), at: www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

32. *See* Cox, Anna Marie, "Why have so Many Liberals Been Silent About NSA Spying?" the Guardian (Aug. 2, 2013), at: www.theguardian.com/commentisfree/2013/aug/02/nsa-spying-liberals-presidential-candidates-silent.

the fear of being spied on."[33] And to attempt a clinical observation of the long-term effects of surveillance would be morally repugnant – rendering the subject little more than a human toy.

In reality, of course, none of us who have been even remotely engaged on issues of security and privacy had until June 5, 2013 been living in a state of blissful naiveté. Many of us assumed that in some way, shape or form, we were being surveilled for purposes of national-security. The issue, though, is the degree to which needs for intelligence have – since 9/11 – progressively weighed far more heavily in the balance with privacy and civil rights. For better or worse, I spent a greater part of the nine months after June 5 writing, speaking and providing commentary on issues relating to the surveillance revelations. My analysis of the legal issues is best left to other texts, particularly a speech I gave at the International Bar Association conference in Boston in October 2013.[34] Suffice it to say that the same "many of us" who presumed some measure of surveillance as a necessity, also assumed that there were far greater limits, audits to show justifications, and oversight.

We need only look to the two reports issued in December 2013 and January 2014, from the President's Review Group on Intelligence and Communications Technologies (PRG-ICT)[35] and the Privacy and Civil Liberties oversight board (PCLOB),[36] respectively, to

---

33. *Ibid*.

34. *See generally* Boam, Chris, "How the Net was Won: Internet 2.0 – to Regulate or Not to Regulate," a panel event of the International Bar Association Annual Conference (Boston, Mass.) (Oct. 10, 2013), at: www.40a-m.com/uploads/3/1/9/0/3190984/iba_cboam_10oct2013.mp4 (conference audio and slides) and www.40a-m.com/uploads/3/1/9/0/3190984/iba_-_cboam_-_2013-10-10.pdf (slide set only); *see also* Boam, *supra* note 29.

35. *See* President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, (Dec. 12, 2013), at: www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

36. *See* Privacy and Civil Liberties Oversight Board (PCLOB), Report on the Telephone Records Program Conducted Under section 215 of the U.S.A. Patriot Act and the

know that we were wrong. For instance, the PCLOB determined that the mass surveillance program was not only ineffective, but also, had no basis in law. It also found that the program had never stopped even a single imminent terrorist attack. The greatest success that the program had produced was the discovery of a taxi driver in the U.S. who had been transferring USD 8,500 dollars to Somali contacts in 2007.[37] For the many millions in resources that have been spent on "collecting it all" and developing technologies to parse the minutiae of so many daily lives – what are we missing? Are there fewer traditional intelligence investigations running down real leads?

And what have been the economic trade-offs? By early August 2013, the Information Technology & Innovation Foundation (ITIF) had published a brief[38] outlining potential impact to the U.S. cloud computing industry. Out of a global enterprise cloud computing market of USD 207 billion, ITIF suggests that by 2016, U.S. cloud providers could lose USD 35 billion.[39] Technology commentator James Staten analyzed the ITIF efforts and found them excellent, but perhaps underplaying the impact, suggesting that the loss could be as great as USD 180 billion or a 25% hit to overall IT service provider revenues in that same timeframe.[40] Still others are trying to take the pulse of broader consumer concerns, with one outlet reporting in mid-August 2013 that after only seven weeks of post-

---

Operations of the Foreign Intelligence Surveillance Court, (Jan. 23, 2014), at: www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

37. *See ibid*. at 156 § D.

38. *See* Castro, Dan, Information Technology and Innovation Foundation, How Much will PRISM Cost the U.S. Cloud Computing Industry? (August 2013), at: www2.itif.org/2013-cloud-computing-costs.pdf.

39. *See ibid*.

40. *See* Staten, James, "The Cost of PRISM will be Larger than ITIF Projects," Forrest Research (Aug. 14, 2013), at: blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

Snowden media coverage, the percentage of Internet users reporting concerns about their privacy online jumped from 48% to 67%.[41]

4. WHERE DO WE GO FROM HERE?

More recently, I have seen some take the view that privacy is less "dead" than a victim of circumstance – run over by the unstoppable train of data use and collection that is riding the rails of humanity's "hunger for information" and the "need to know more." The "gotta have it" view seems too dystopian a rationale for the much needed revisiting of key privacy compliance concepts, such as the nature and quality of consent and a more dynamic view of when it is required. We need to give the advance of "big data" and all of its potential benefits – and certainly the consumer – far more credit.

Only five years ago, I remember briefing a Member of the U.K. Parliament on the "internet of things" who, though very tech savvy, drolly remarked that, "if my refrigerator could tweet, I'm not sure that I would want to see what it said." In five years, we have come a long way. In a speech at the Woodrow Wilson School of Public and International Affairs, Commissioner Julie Brill of the U.S. FTC highlighted just some of the many ways in which the cloud, big data and analytics are beginning to change our lives in profound and beneficial ways:

> by addressing important societal issues like keeping kids in high school; conserving our natural resources by making our use of electricity more efficient; providing first responders in crisis situations with real-time information about the injured or those who lack power, water, or food; and performing other miracles in the health care sector. Indeed, the opportunities big data analytics may provide in the field of medicine are staggering: prevention of infections in premature children, mobile apps that

41. *See* "Study: NSA Scandal is still Setting off Privacy Alarm Bells Among Consumers," Adweek (Aug. 13, 2013), at: www.adweek.com/news/technology/study-nsa-scandal-still-setting-privacy-alarm-bells-among-consumers-151835. *See also* Cobb, Stephen, "NSA Revelations Shake Faith in U.S. Tech Firms as Harris Poll Shows Public Conflicted," WeLiveSecurity.com (Apr. 9, 2014), at: www.welivesecurity.com/2014/04/09/nsa-revelations-shake-faith-in-tech-u-s-firms-as-harris-poll-shows-public-conflicted/.

> distribute information to clinicians about bacteria types and resistance patterns in relevant communities, and the development of preventive programs that anticipate a person's health status.[42]

I agree with Daniel Weitzner, former Deputy White House Chief Technology Officer for Internet Policy and now Director of the MIT CSAIL Decentralized Information Group, who recently noted in an interview that there is a tendency in the U.S. to believe that you can only have privacy if you have secrecy – that "if third parties hold your personal information, then somehow you've lost all your privacy."[43] This is, in part, an outgrowth of the 1967 decision of the Supreme Court in *Katz v. U.S.*[44] In *Katz*, John Marshall Harlan's concurring opinion established the "reasonable expectation of privacy" test, which contains a subjective component (actual expectation of privacy) and an objective component (reasonable expectation of privacy). It was the objective element that has had the unfortunate distinction of evolving into what has become known as the "third party doctrine" in the U.S. – by which one diminishes or even loses an expectation of privacy through voluntary turnover of data to a third party.

Increasingly, it is the quality of "voluntarism" that is the key component in the doctrine. As Mr. Weitzner notes, "protecting privacy in the digital age means creating rules that require governments and businesses to be transparent about how they use our information."[45] This is likely the most important way in which our address of privacy

---

42. Brill, Julie – Commissioner, Federal Trade Commission, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions," Address at the Woodrow Wilson School of Public and International Affairs, Princeton University, (February 2014), at 4, at: www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf.

43. *See* Henn, Steve, "If there's Privacy in the Digital Age, it has a New Definition," Nat'l Public Radio – All things Considered, (Mar. 3, 2014), at: www.npr.org/blogs/alltechconsidered/2014/03/03/285334820/if-theres-privacy-in-the-digital-age-it-has-a-new-definition.

44. *See* 389 U.S. 347 (1967).

45. *See* Henn, *supra* note 43.

must evolve. Transparency needs to be concise, meaningful and useful. And, while the need for a clear "check box" of consent is – for lawyers – a holy grail on both Atlantic coasts, consumers (and their choices) far too often fall down the rabbit hole of interminable language as they pull the lever saying, "I agree." This treads upon the notion of what is or is not truly "voluntary" under the *Katz* and its progeny.

I am in full agreement that it is time in the U.S. for adoption of baseline privacy legislation for the commercial sector, as Commissioner Brill has said, "to close the gaps in consumer privacy protections and help level the playing field among businesses."[46] A key new component, or companion legislation – as Commissioner Brill highlights – should require data brokers to "provide notice, access, and correction rights to consumers scaled to the sensitivity and use of the data at issue."[47] This is an area where Daniel Weitzner also seems to be in agreement. He "envisions a world where big databases are audited to prevent abuse, including those at the NSA, and where encryption technology ensures that research involving troves of sensitive personal information don't open windows into individuals' personal lives."[48]

The drive for over-arching privacy legislation in the U.S., to supplant or supplement the sector-by-sector approach of our present rules, is in no small measure an outgrowth of the current debate over surveillance measures. We do not have to pass judgment on revelations about the NSA to know that these have not only spurred an overdue debate, but also, may already be altering the way we think about communications technologies in ways that may take years to fully realize or understand.

For these reasons, I applaud President Obama for welcoming the debate that has developed in the wake of the surveillance revelations and his January 17, 2014 speech at the Department of Justice calling for reforms. As I write, the White House and Congress are both poised to introduce legislation to recommend an end to the NSA's bulk phone meta-data collection program, in favor of commercial retention of that same data for an eighteen-month period. This is a duration that most telecommunications providers

---

46. *See* Brill, *supra* note 42, at 8.

47. *See ibid*.

48. *See* Henn, *supra* note 43.

already retain and it is expected that the NSA would be required to produce a court order to access it.

But I also applaud the President for calling for a "national conversation" about big data sets, because the conversation must not be restricted to government entities."[49] In this regard, I was pleased that Commissioner Brill noted in her speech that:

> leaders within the business community have joined the President in recognizing that rebuilding the trust of individuals is essential to the success of all programs and services – both governmental and commercial – built on big data analytics. These business leaders have urged companies to adopt enhanced privacy protections as a key part of strengthening consumer trust.[50]

This is not, however, an area of trust where the U.S. stands alone with work to do. I was not surprised by Christopher Wolff's revelation in March 2014 that European Parliament Rapporteur Jan Philipp Albrecht is also wary of EU Member State surveillance tactics that raise privacy concerns.[51] The draft European Parliament report on mass surveillance had contained a directive specifically that: "the UK, France, Germany, Sweden, the Netherlands and Poland should clarify the allegations of mass surveillance and their compatibility with EU laws."[52] Several privacy experts in the U.S. have also argued effectively that the U.S. is not alone in terms of its surveillance modes and

---

49. *See,* e.g.*,* Byers, Alex, "How to Woo Silicon Valley," Politico Morning Tech, (Jan. 21, 2014), at: www.politico.com/morningtech/0114/morningtech12767.html.

50. *See* Brill, *supra* note 42, at 6.

51. *See* Wolff, Christopher, "My Dinner with Jan," IAPP Privacy Perspectives, (Mar. 18, 2014), at: www.privacyassociation.org/privacy_perspectives/post/my_dinner_with_jan.

52. *See* European Parliament, "Q&A on Parliament's Inquiry into Mass Surveillance of EU Citizens" (updated Mar. 10, 2014), at: www.europarl.europa.eu/news/en/news-room/content/20140310BKG38512/html/QA-on-Parliament%27s-inquiry-into-mass-surveillance-of-EU-citizens.

methods.[53] Though the "everybody's doing it" and "our law is better" arguments from the U.S. on these issues may not be dispositive of big problems, they certainly have provided helpful perspective and hopefully tempered some hyperbole.

The real danger of a surveillance state is a person or persons who believe(s) that the broadening of authorized surveillance actions is always morally justified and prudent. It is someone who, perhaps with the best of intentions, can make the most grievous of mistakes with eyes wide open and believe that the ends do justify the means.[54]

The maintenance of dignity through privacy is ultimately about defining one's autonomy within a society. It is the boundary between the individual and society. The fact that Adam and Eve were aware of their nakedness, and ashamed of it, is in the Christian sense cited as a by-product of their "original sin." But in a larger sense, their defenses to shame arose from recognition of power – in this example, God's power – and the feeling of smallness in recognition of it, the vastness of their environs and what they knew or did not know. Circumstances had suddenly made them self-aware in a brave new world. Sound familiar? I agree with those taking an extreme view on the "death" of privacy to the extent that the innovation of the digital age and all that it will do to change and enhance our lives will alter forever how we think about communities and the maintenance of standards. It must. The promise of the digital age and its improvement of society on so many levels have not, however, also metaphorically erased the requisite for dignity. Not even the internet is that creatively destructive.

---

53. *See,* e.g.*,* Wolf, Christopher, "Is Personal Data Better Protected from Surveillance in Europe than in U.S.? Maybe not," Privacy Perspectives (Jun. 20, 2013) at: https://www.privacyassociation.org/privacy_perspectives/post/is_personal_data_better_protected_from_government_surveillance_in_europe_th; Baker, Stewart, "Intelligence Under Law: Judiciary Testimony," SkatingOnStilts (Jul. 16, 2013), at: http://www.skatingonstilts.com/skating-on-stilts/2013/07/nsa-fisa-surveillance-stewart-baker.html.

54. *See* Khanna, Derek, "If PRISM is good policy, why stop with terrorism?," The Atlantic (Jul. 4, 2013), at: http://www.theatlantic.com/politics/archive/2013/07/if-prism-is-good-policy-why-stop-with-terrorism/277531/.

The question of whether and under what circumstances we champion privacy – as a right, as a freedom to be left alone, as a concept embodied in an over-arching omnibus law, or as merely a protection that we want afforded by the court in response to a harm – raises much larger issues of what kind of society we want to be and how we prioritize our freedoms versus our restrictions. If we truly believe that privacy is lost, then a key component of what makes us human is as well.