Kift, Paula

Article

To have or not to have: the true privacy question

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Kift, Paula (2013) : To have or not to have: the true privacy question, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 2, Iss. 4, pp. 1-7, https://doi.org/10.14763/2013.4.223

This Version is available at:
https://hdl.handle.net/10419/213979

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 2 | Issue 4

To have or not to have: the true privacy question

Paula Kift
Global Public Policy Institute, Berlin, Germany

Published on 03 Dec 2013 | DOI: 10.14763/2013.4.223

Abstract: In light of the recent US National Security Agency (NSA) surveillance scandals, the article reflects on the continued importance of privacy in the information age. Based on a taxonomy of privacy violations provided by Daniel Solove, it takes the reader on an imaginary journey to a world in which privacy has ceased to exist. What does it mean "to have or not to have privacy" in the information age? This essay, part academic, part call for action, explores this question by means of an analogy, focusing on the relationship between citizens and the state. It demonstrates that the invisible presence of the NSA should be a matter of great concern to us. There is no justification for blanket surveillance. The right to security is an illusion. Instead of fighting windmills, we should fight for our right to privacy instead. We need to have privacy; we need it to live and love, to make mistakes, and to grow. We need it as individuals and as a society. And we can have it if we press our legislators to return it to us. It is time to start fighting back.

Keywords: Blanket surveillance, Privacy

Article information

Received: 13 Oct 2013 **Reviewed:** 27 Nov 2014 **Published:** 03 Dec 2013

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/have-or-not-have-true-privacy-question

Citation: Kift, P. (2013). To have or not to have: the true privacy question. *Internet Policy Review*, *2*(4). DOI: 10.14763/2013.4.223

If you do not see a policeman outside of your door, you are looking out of the wrong window. An analogy of privacy violations.

THE ABYSMAL CONCEPT

What is privacy and why does it matter? Scholars have been struggling to find a universal answer to these questions ever since Warren and Brandeis published their famous article on the "Right to Privacy" in 1890, lamenting the intrusions of press and media into the personal lives of US American citizens. But not even in their darkest dreams would Warren and Brandeis have imagined the kinds of privacy invasions made possible today. The internet has elevated the scale

and scope of personal data mining to formerly unprecedented levels. The recent surveillance scandals[1] are but an example of how public and private actors readily exploit the literally boundless availability of personal information online.

We are left with a feeling of vague unease. We are afraid of losing our privacy. And yet we struggle to define what that even is. As Daniel Solove once deplored: "Privacy is a concept in disarray. Nobody can articulate what it means" (2006, p. 477). He has a point. After all, when we worry about privacy, is it our physical privacy, thus our right to solitude and isolation that we are concerned about? Or should we rather fret about our informational privacy, thus our right to data privacy, secrecy and confidentiality? Proprietary as well as decisional privacy further add to the terminological pandemonium (Allen, 1999, p. 723-24); more recent contributions include up to seven different classifications of privacy (Finn et al., 2013). But even if we were able to answer all these questions for ourselves, the singularity of our privacy needs would necessarily preclude us from daring to make any generalisations (cf. Nissenbaum, 2004). What, then, makes us frantically cling on to a concept whose proper meaning we cannot even functionally elucidate? If economics is the abysmal science, then I suggest that privacy might very well be called the abysmal concept.

Perhaps it does not matter. After all, "many things have well-established but inappropriate names – for example, the Holy Roman Empire, which, as Voltaire pointed out, was neither holy, nor Roman, nor an empire" (Oppy, 1995, p. 1). The Holy Roman Empire nevertheless existed or at least we realised that it once had as soon as it fell apart. *Don't it always seem to go, that you don't know what you've got til it's gone*, Joni Mitchell sang to us in 1970. The same may well hold true for privacy. Therefore, rather than wasting our words on the futile undertaking of understanding what it means to have privacy, I propose we should devote more attention to the curious state of affairs we would encounter if we did not. Indeed, to have or not to have – that is the true privacy question.

PRIVACY RIGHTS AND VIOLATIONS

Solove was right on track. As he gave up on defining what it meant to have privacy, he started thinking about the different ways in which it could be taken away from us. Solove did not attempt a taxonomy of privacy but rather a taxonomy of privacy violations. According to Solove, privacy violations fell within four broad categories: invasion, collection, processing and dissemination. Each category can then be further subdivided (Solove, 2006). However, while it may be easy to imagine privacy violations in everyday life, information technologies complicate conceptualisation. We perceive a difference between somebody opening our mailbox and tearing open all our letters, and somebody tacitly scanning our email exchanges from afar; the physical invasiveness of the former makes the privacy violation more tangible, while the faraway gaze of the latter seems less intrusive. There is a "threshold of abstraction" (Székely, 2010, pp. 167-68), so to speak.

Indeed a study on online privacy concerns conducted at Humboldt University in the fall of 2012 revealed that while university students expressed concern about their privacy online, they were incapable of formulating the origin and nature of their fear (Krasnova and Kift, 2012). However, if we want to change the course of politics, we need to understand what blanket surveillance actually implies. What does it mean 'to have or not to have privacy' in the information age? I would like to explore this question by means of an analogy, focussing on the relationship between citizens and the state.[2]

TO HAVE OR NOT TO HAVE: AN ANALOGY

INVASION

Imagine that every day, in front of every house, there was a police officer. He does not talk to you, he does not bother you, he is merely present. In fact, his presence is so inconspicuous that you barely notice him. What does this policeman do? He stands in front of your house and watches you. He watches every person entering and leaving your house, the friends and neighbours with whom you chitchat on the street, the greengrocer who delivers local vegetables once a week. Of course, you need not worry about him. After all he is only there to increase your safety. If you have nothing to hide you have nothing to fear[3]. Little does it matter that you are a well-intentioned law-abiding individual. The policeman is out there for people who *seem* good but *could* be bad. Just like Google, he wants to know the answer before you know the question (Miller, 2013). He is there to protect citizens like you. But would his continuous presence make you feel uncomfortable? It probably would. He has crossed the boundary of the first of Solove's privacy violations, namely invasion. He is a stranger who has entered your private sphere.

COLLECTION

But let us take the analogy a step further. Imagine the policeman would not only watch your relationships but also take note of them. Every day, he records the interactions you have with your surroundings. He does not listen to your conversations but he knows when, with whom and how often you talk. He recognises your husband and children by now and he has figured out that the old lady who brings over cake once a week is your mother. Your good friend Susan is clearly the mother of a classmate of your son at school, as the former often picks up the latter from your house. The policeman sees all of that. The only interaction that may seem a little strange is the one you have with your colleague John at work, who seems to only come around when your husband is on a business trip. Sometimes John only leaves in the morning. But of course you need not be bothered that the policeman knows of your extramarital affair since that is not the kind of information he is looking for. And of course it is only in his professional records to which only he and perhaps another couple hundreds or thousands of his colleagues have access (Lennard, 2013). But no worries, all the information is kept confidential. Would his knowledge nonetheless disturb you? It probably would. The policeman has crossed the boundary of Solove's second privacy violation, namely collection. He is a stranger who is collecting information about you.

PROCESSING

But of course the story does not end there. As any good policeman he has to be alert. What if your interactions become suspicious? Imagine you were interested in buying a new pressure cooker. You have a chat about it across your garden fence with your neighbour. The policeman takes note of it. At the same time, your husband is looking for a new backpack and equally asks around. This is when alarm bells should start ringing. This interaction seems innocent to you? Thankfully, we have men and women working for our police departments who are acutely aware of the danger of the search combination of pressure cookers and backpacks. Did you know that pressure cookers are not only helpful for cooking rice but also for building bombs? And that bombs are often transported in backpacks? Of course, if you are aware of this information it seems much more justified if six officers from a joint terrorism task force show up in front of your door and ask you where you are from, where your parents are from, where your parents live and where you work.

Do you own a pressure cooker? No, but we own a rice cooker. *Can you make a bomb with that?* No, but we use it to make quinoa. *What the hell is quinoa?*

Would their questions anger you? They probably would. But the policemen are just doing their job. A hundred false alarms are better than one real one. Do you not agree? You do not?

DISSEMINATION

What has become of your privacy at this stage? The policeman knows when, with whom and how often you speak and, he keeps track of this in an enormous database. He draws connections between the content of your conversations and the people with whom you converse. He knows about your marriage and your extramarital affairs. He also knows that you like to travel and eat quinoa.

It used to be you who chose with whom to share this information. But of course we cannot afford this kind of luxury anymore in the information age. We are permanently threatened, we *need* to fear. Sharing our whole lives with the police is just the price we need to pay for our safety. Our right to privacy was replaced with a right to security. Was our intimacy replaced with an illusion?

Again: What has become of your privacy? Perhaps you are still not concerned. Perhaps you are not even bothered. After all, the information is kept confidential. All your information is stored in the same place, accessible only to the police. How convenient. But is it not convenient for criminals too? What if somebody could access the system? It seems unlikely. Policemen are professionals after all; they take great care of the security of your information. The system may not be bulletproof. But again the likelihood is low that somebody would be able to steal your information and use it for criminal purposes; criminal purposes such as blackmailing you about your love affair with your colleague and threatening to go public with it. If the latter were to happen, that would of course be unfortunate. Would the incidence devastate you? It probably would. The last frontier of Daniel Solove's privacy violations would be breached. Your information has been disseminated and entered the uncontrollable unprotected unpredictable public sphere.

O PRIVACY, WHERE ART THOU?

But how does all of this relate to you? The last time you looked out of your window there was no policeman standing in front of your door. *But perhaps you were looking out of the wrong window*. The NSA is not guarding your door; it is checking your inbox (Gellman and Soltani, 2013, October 15; Gellman and Soltani, 2013, October 30; Glüsing et al., 2013). Your metadata reveals exactly when you communicate, with whom and how often. If you continuously communicate with one contact, this contact will appear suspicious[4]. This contact could be your extramarital affair. But it could also be a criminal lead. Do you still believe that if you have nothing to hide you have nothing to fear? Did the story about the pressure cooker and backpack seem implausible to you? It was not a story. It happened to Michele Catalano, resident of Suffolk County in the State of New York, in August 2013. Catalano had searched for a pressure cooker, her husband for a backpack online, following which Suffolk County Police Detectives came around for a visit. The conversation cited above is a direct quote from the interaction (Bump, 2013). The Suffolk County Police Department had indeed never heard about quinoa. But it had heard of backpacks and bombs. *Monitoring our Google searches and email exchanges is far worse today than waiting in front of our doors*. How many times have you spoken to your

neighbour today? And how many emails have you sent? Chances are, that the majority of your interactions take place online; on your laptop, your tablet, your smartphone. Just because you cannot see the NSA does not mean it is not there. Its invisible presence should be a matter of grave concern to you. It certainly already is to me. There is no justification for blanket surveillance. There is no proof it is effective. It cannot be. There is no such thing as a right to security. Life will always be beyond our control. Intrusions are only justified by threat. And threats need to be substantiated by more than mere possibility. *If searching for a terrorist is like searching for a needle in the hay, then what the NSA is doing is just adding more hay* (Mueller and Stewart, 2013). So instead of fighting windmills, we should fight for our right to privacy instead. We need to have privacy; we need it to live and love, to make mistakes, and to grow. We need it as individuals and as a society. And we can have it if we press our legislators to return it to us. Closing your eyes and hiding under the bed will not make the monsters go away. It is time to start fighting back.

FOOTNOTES

1. On June 6, Guardian journalist Glenn Greenwald published the first of a series of articles focused on secret surveillance programmes conducted by the National Security Agency (NSA) in the United States and the Government Communications Headquarters (GCHQ) in the United Kingdom. The documents were provided by whistleblower Edward Snowden. For a chronology of the events, see Lütticke, 2013.

2. While it is outside the scope of this article, it should be mentioned that the issue of privacy could and should also be analysed in the context of violations performed by non-state actors, such as IT, medical and insurance companies, just to name a few.

3. For a more in-depth discussion of the fallacy of the "nothing to hide, nothing to fear" argument, see Solove, 2007.

4. For an impression of what kind of information metadata reveals about you, try logging into the MIT Immersion program with your Gmail account: https://immersion.media.mit.edu/

REFERENCES

Allen, A. (1999). Coercing Privacy. *William and Mary Law Review*, 40(3).

Bump, P. (2013). The Atlantic Wire. *Update: Now We Know Why Googling 'Pressure Cookers' Gets a Visit from Cops*. Retrieved October 13, 2013, from http://www.theatlanticwire.com/national/2013/08/government-knocking-doors-because-google-searches/67864/.

Finn, R., Wright, D., & Friedewald, M. (2013). Seven Types of Privacy. In: Gutwirth, S. et al. (eds.). *European Data Protection: Coming of Age*. New York/Heidelberg (pp.3-32). Springer.

Gellman, B., & Soltani, A. (2013, October 15). Washington Post. *NSA Collects Millions of E-Mail Address Books Globally*. Retrieved November 15, 2013 from http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-email-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

Gellman, B., & Soltani, A. (2013, October 30). Washington Post. NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say. Retrieved November 15, 2013 from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

Glüsing, J., Poitras, L., Rosenbach, M., & Stark, H. (2013, October 20). Spiegel Online. *Fresh Leak on US Spying: NSA Accessed Mexican President's Email*. Retrieved November 15, 2013 from http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

Krasnova, H., & Kift, P. (2012). Online Privacy Concerns and Legal Assurance. *Pre-ICIS workshop on Information Security and Privacy (SIGSEC)*.

Lennard, N. (2013, August 1). Salon. *500,000 Contractors Can Access NSA Data Hoards*. Retrieved October 13, 2013 from http://www.salon.com/2013/06/11/500000_contractors_can_access_nsa_data_hoards/.

Lütticke, M. (2013). Deutsche Welle. *A Chronology of the NSA Surveillance Scandal*. Retrieved November 15, 2013 from http://www.dw.de/a-chronology-of-the-nsa-surveillance-scandal/a-17197740.

Miller, C.C. (2013, July 29). New York Times. *Apps That Know What You Want, Before You Do*. Retrieved October 13, 2013 from http://www.nytimes.com/2013/07/30/technology/apps-that-know-what-you-want-before-you-do.html?pagewanted=all&_r=0.

Mueller, J., & Stewart, M.G. (2013, June 13). The Chronicle of Higher Education. *3 Questions About NSA Surveillance*. Retrieved November 15, 2013 from http://chronicle.com/blogs/conversation/2013/06/13/3-questions-about-nsa-surveillance/.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79(1).

Oppy, G. (1995). *Ontological Arguments and the Belief in God*. Cambridge, UK: Cambridge University Press.

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3).

Solove, D. (2007). "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review*, 44.

Székely, I. (2010). Changing attitudes in a changing society? Information privacy in Hungary 1989–2006. In: Elia Zureik et al. (eds.). *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons*. Montreal, Kingston, London, Ithaca: McGill-Queen's University Press: pp. 150–170.

Warren, S.D., & Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5).