GlobalResearch
Center for Research on Globalization

Does Mass Surveillance Change the Way We Behave? "Privacy Data" Collected on a Global Scale

Are You Looking at Me? Are You Looking at Me Looking at You?

By Boen Wang
Global Research, December 04, 2015
Who.What.Why. 1 December 2015

Region: Europe, USA
Theme: Police State & Civil Rights

On Sunday, the NSA was forced to shut down its bulk collection of the phone records of Americans. While that program may have ended — and there is evidence that it may not have — the world now knows the spy agency's capabilities, and that is changing the behavior of people everywhere.

How much, and in what way, is currently being studied. What effect does the awareness of surveillance have on the behavior of people? *WhoWhatWhy* looked at the available results of research being conducted, and found that we may be reaching the tipping point — when awareness of being watched starts to affect behavior.

Helsinki Syndrome

A team of researchers from the Helsinki Institute for Information Technology recorded nearly every piece of data — calls, texts, GPS locations, keypresses, mouse clicks, screenshots of computer desktops, browsing histories, and credit card usages, a total of 32 TB of data from 10 households — for an entire year. They found that constant, intrusive surveillance consistently resulted in behavioral effects.

> As Oulasvirta explained, "people may stop being careful after they have slipped at least once. Digital records that are not erased will contain that slip (potentially) for a long time."

The researchers called the study "The Helsinki Privacy Experiment," and in September 2012 they published their findings in the paper, "Long-term Effects of Ubiquitous Surveillance in the Home."

Interestingly, the researchers found that increased surveillance did not necessarily increase stress.

However, Antti Oulasvirta, lead author and electrical engineering professor at Aalto University, warned against jumping to conclusions based on the above. "You have to remember that they self-selected themselves to the study, consented, and knew how the data is going to be treated and used. This is not the case with the NSA, for instance," he told *WhoWhatWhy*.

While there were few psychological impacts, researchers found significant changes in subjects' behavior.

Some spent more time in rooms that weren't covered by cameras, while others retreated to cafes and libraries to discuss private matters and browse the internet undetected. Having guests over was a particular source of anxiety, as Finnish law requires signs outside areas with camera surveillance. Some subjects admitted to turning off the cameras during social events rather than explaining the study to friends.

Subjects also wore more clothes at home and avoided intimate interactions in surveilled areas, though some described becoming accustomed to the camera's presence. "After I realized that I'd already walked naked to the kitchen a couple of times, my threshold kind of got lower after that," one participant said in the paper.

In effect, inadvertent disclosures of compromising images or information eventually made the participants less sensitive about such disclosures. As Oulasvirta explained, "people may stop being careful after they have slipped at least once. Digital records that are not erased will contain that slip (potentially) for a long time."

Not all of the subjects were comfortable with the experiment. One participant became increasingly disturbed by the surveillance and dropped out after six months. Constantly being observed, the subject said, in notable understatement, was "not fun."

Pipe Bombs and Kardashians

What if vast quantities of data were collected on a global scale?

Boston-based privacy advocate Alex Marthews and MIT professor Catherine Tucker analyzed search data from 11 different countries (the US and its top ten trading partners) from Google before and after June 6, 2013 — when the media revealed the existence of PRISM, the NSA's internet communications collection program. According to their working paper, "Government Surveillance and Internet Search Behavior," awareness of government surveillance of one's search behavior on the Internet had a "chilling effect."

The investigators analyzed the use of three sets of search terms: (1) those that could get the user in trouble (e.g., "pipe bomb," "anthrax"); (2) terms that were considered personally embarrassing (e.g.,"white power," "sexual addiction"); and (3) a non-worrisome control group of terms for comparison: Google's top 50 search terms for 2013 (e.g., 2014 FIFA World Cup," "Kim Kardashian baby").

They found that — after June 6, 2013 — users were less likely to search for terms they believed might get them in trouble with the US government. That, naturally, had a more pronounced effect in the US, while other countries saw a more significant drop in use of terms that might prove personally embarrassing.

***

But a May 2015 paper called "Privacy Behaviors After Snowden" seems to contradict Marthews and Tucker's conclusions. It found a more carefree attitude toward a loss of privacy.

Google researcher Sören Preibusch, who worked for Microsoft when he wrote the paper, analyzed Bing search data for PRISM-related terms ("Snowden" and "NSA"), pageviews for PRISM-related topics (Microsoft's privacy policy page and various Wikipedia articles), and

the use of privacy-enhancing tools (the Firefox extension*Anonymox* and the *Tor* internet browser).

> This deeply troubles Titus. As he puts it, a person is a collection of data points that can be thought of as a "digital soul, a thing that is you, but yet can be disembodied from you and still exist." Legally speaking, data in the US is considered property, and if "we are data, and if data is property, then we are property."

They concluded that the PRISM revelation "had only a small impact on Web users beyond debates among journalists and academic researchers." And Marthews noted that Preibusch used data from Bing, and that "Bing users may differ from average internet users."

The Tipping Point

What Marthews and Preibusch both agree on is that more research needs to be done. One researcher, Iowa State business professor Brian Mennecke, is looking into what he calls the privacy "uncanny valley," — the tipping point at which surveillance becomes sufficiently "creepy" to result in behavioral change.

"What makes something creepy?" Mennecke told *WhoWhatWhy*. "I don't know the answer right now, but it's an important question."

Mennecke primarily studies corporate applications of surveillance. These include video analytics technology, where digital signs can, for example, analyze a person "based on their clothing, how they walk, height, hair color" — and pitch specific ads to him or her. This technology is already available: NEC has software that "automatically detects suspicious behavior such as intrusion, loitering, and object abandonment," according to its website.

Iowa State PhD student Akmal Mirsadikov posed another example: Walmart experimenting with facial recognition software, where cameras scanned the faces of customers, compared them to a database of known shoplifters, and alerted security personnel if a match was found.

When this type of technology is announced, "people freak out. We want to find out why that happens," Mirsadikov told *WhoWhatWhy*.

One factor that could affect behavior because of awareness of surveillance is what Mirsadikov called the "saliency" of surveillance. "For example, let's say death. That is inevitable. Everybody takes it easy because you cannot always live worrying about death. But if a doctor says you have cancer and you only have a few days left, you suddenly become very aware of this, and your behavior changes very suddenly," Mirsadikov said, implying that, perhaps in the same way, sudden shocks about mass surveillance could trigger unease that results in altered behavior.

Digital Souls

We may have already crossed the tipping point, says Aaron Titus, former privacy director of the Liberty Coalition. Most of us, Titus told *WhoWhatWhy*, have a vague notion that we are being surveilled, but don't understand how much, or in what way it affects our lives. And there is no incentive to find out.

This deeply troubles Titus. As he puts it, a person is a collection of data points that can be thought of as a “digital soul, a thing that is you, but yet can be disembodied from you and still exist.” Legally speaking, he said, data in the US is considered property, and if we are data, and if data is property, then we are property.

The need for privacy, then, is not just a matter of control over who can see one’s Facebook profiles, but control over one’s self. Addressing the notion that privacy doesn’t matter if one has nothing to hide, he said that implies that shame is the only reason anyone would want privacy.

Privacy is necessary he said, “because individuals and institutions do not act in the best interest of other individuals, institutions, or society at large, when in possession of true facts.”

For example, people keep their social security numbers private, not because they are ashamed of them, but because of what thieves can do with them. The idea that a central power would act in society’s best interests if it had access to everyone’s information is, according to Titus, demonstrably incorrect.

“I wish we could see…that we’re living in a panopticon. Then at least it would spur us on to some sort of action,” Titus said. The image is compelling: a panopticon is a circular prison with cells arranged around a central well from which prisoners can be observed at all times.

“My personal opinion is that privacy is going to lose, or at least it’ll take another generation, and at least some major event, before privacy really becomes something that is concrete again to fight for.”
