The NSA/Prism firestorm: Will personal privacy become a thing of the past?

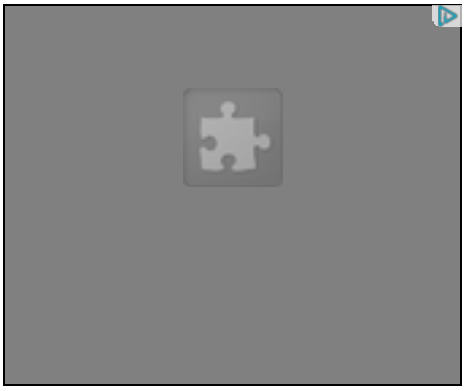
by **Chandra Steele**, *09 July, 2013*

This might be the end of the end of privacy. By releasing one warrant, four slides, and a few minutes of video about his motivation for doing so, Edward Snowden has opened up a **firestorm of debate** about what personal data is out there – and who's looking at it.

We confess our most private thoughts to search engines, broadcast our location for free drinks, let our cars be tracked for an insurance discount, and snap

1

"sexts" trusting they'll be deleted, yet now we find ourselves suddenly howling with outrage over our privacy.



The fact that two major entities – government and multinational corporations – are interested in data comes as no surprise. What has been a jolt is just how much data is shared between them over in the US.

Documents from Snowden detailed a secret court order compelling US network Verizon to give the National Security Agency (NSA) its call records, and a still shadowy program called PRISM, in which gatekeepers of private communication – Google, Microsoft, Apple, Facebook, Yahoo, and Skype among them – have been handing over vast quantities of data to the NSA.

Two of a kind

The *New York Times* has highlighted the revolving door between Silicon Valley and the US government; in 2010 Facebook's then chief security officer Max Kelly **left the company to work for the NSA**. At other times the affinity was merely suspected, such as last year when Skype introduced supernodes to improve performance – and, many believed, to **allow easier access for law enforcement**.

Silicon Valley and the US government's interest in data increasingly overlaps. Just three years ago, **Google reached out to the NSA** for assistance investigating an attack believed to have originated in China that targeted Chinese human rights activists' Gmail accounts. When the Electronic Privacy Information Centre filed a Freedom of Information Act request for more details about Google's alliance with the NSA, a **federal appeals court upheld the government's right to keep it secret**.

Despite these past ties, many companies named in the PRISM leak have challenged Snowden's assertions. First of all, we heard their near-universal, carefully worded (and extremely similar) denials that the NSA has direct access to their servers, as depicted in the slides used for training NSA analysts. Then Facebook, Apple, Microsoft, and Yahoo disclosed the number of customer data requests they've received overall (without NSA requests broken out, which are classified). Google is petitioning the NSA for the right to reveal the specific number of requests it's received. In a Congressional hearing at the White House, several Congressmen, and the NSA, stressed that the Verizon data does not include the content of calls, which is true as far as it goes, but omits **how much about you can be determined by metadata**, including your relationships and habits.

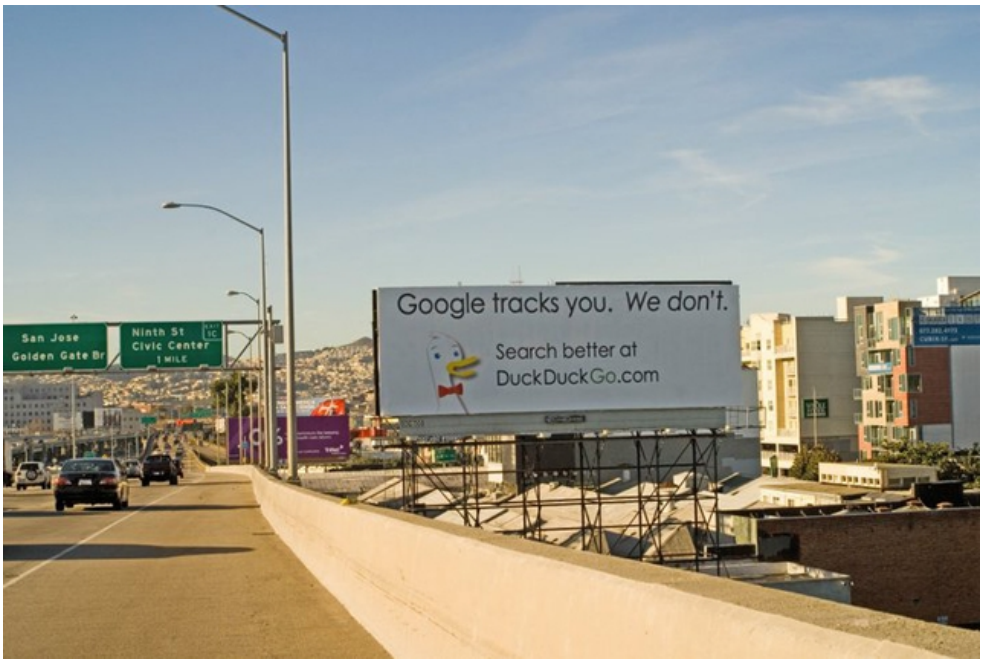
In an **open forum Q&A on the Guardian site**, Snowden held firm to his initial charges that the collaboration between tech companies and the NSA is more extensive than either have admitted. But while the extent to which they collude is in contention, the public is pushing back.

Public opinion

A **Pew Research Centre and *USA Today* poll** found 63 per cent of Americans would feel their personal privacy was violated if they found out the government was collecting their data. Those under 30 and Tea Party Republicans were particularly supportive of Snowden's leaks and critical of

infringements of their privacy. There are now campaigns hounding the US government to **Stop Watching Us**, **"I Stand With Edward Snowden" rallies**, and a **Rand Paul-led proposed lawsuit** against the NSA.

It's not just government that's feeling the heat. Some of Google's traffic has gone to **privacy-protecting search engine DuckDuckGo**. Founder Gabriel Weinberg noted in an email that traffic has grown 73 per cent since the NSA story broke. That's with minimal advertising on Reddit and 4chan. "We find privacy protection spreads best by word of mouth when people can talk to each other more at length about issues/alternatives," Weinberg said.



Earlier this year, Douglas Rushkoff, media theorist and author of *Present Shock: When Everything Happens Now*, declared his **reasons for leaving Facebook** – data mining being chief among them. "We Facebook users have been building a treasure lode of big data that government and corporate researchers have been mining to predict and influence what we buy and for whom we vote," Rushkoff wrote. "We have been handing over to them vast quantities of information about ourselves and our friends, loved ones and acquaintances. With this information, Facebook and the 'big data' research firms purchasing their data predict still more things about us – from our future product purchases or sexual orientation to our likelihood for civil disobedience or even terrorism."

The point about friends, loved ones, and acquaintances is especially salient after a recent data glitch exposed phone numbers and email addresses uploaded by six million Facebook members, which included information on non-members (or, as Facebook thinks of them, potential members). With Facebook, it's basically a case of *All Your Data Are Belong to Us*, whether or not you belong to the site.

Photo: Nicholas Iverson

Some people are not bothered by the government using their data if they feel it's to keep them safe. A *Washington Post/Pew* poll conducted soon after the NSA revelations found 62 per cent felt that **the investigation of terrorist threats trumps personal privacy**.

Data data everywhere

But even when corporations are not collaborating with the NSA, the data they harvest can harbour more than consumers might be comfortable with. Days before the news broke that Verizon had been regularly turning over communications data to the NSA, the ***Wall Street Journal* published** a story on Precision Market Insights, a unit within Verizon set up to sell customer information. On the same page that **Verizon assures its customers it will protect their privacy**, it tells potential users of their data that it can "isolate where consumer groups work and live, the traffic patterns of a target audience and demographic information about what groups visit particular locations."

Details on how much these consumers have to spend is also for sale. Earlier this year in an NBC News investigation, Equifax, one of the big three US credit-reporting agencies, was found to **sell to "debt collectors, financial service companies, and other entities" human resources information** such as paystub data and "other kinds of human resources-related information" including health care provider and insurance details.

The sale of data of an even more personal nature was made public last year in two US civil lawsuits which revealed that **CVS and Walgreens sold prescription information** (patients' and doctors' names, contact information, and prescription details) to drug companies. Consumers began to suspect the indiscretion when they received pitches from the drug companies.

Even when consumer privacy is protected by law, it takes just one person with access to sensitive data to make it public – as the NSA found out. Where companies are concerned all that needs to be offered is a price. The Federal Trade Commission (FTC) set up a sting this year and found that **data brokers were willing to illegally sell information** to those who provide insurance and employment. 10 out of the 45 brokers targeted by the FTC violated the law and were only sent warning letters. Last year, Spokeo, which is the subject of many a paranoid forward from older family members, paid the FTC a fine of $800,000 (£520,000). It was found to have invited potential employers to "**explore beyond the resume**," but did not properly notify consumers about their rights with regard to their data, and failed to ensure the information would be used within legal purposes, or that it was accurate.

Now that we are becoming explicitly aware of how government is intruding on personal privacy – and not stepping up when corporations do the same, our rights and the limits of our rights are coming into focus. What we do about it remains to be seen.

Topics

security | *features* | *prism* | *nsa* | *edward snowden* | *verizon* | *privacy* | *facebook*

0 Comments

Related Articles

SECURITY

New Snowden documents show Microsoft helped NSA access encrypted messages

16 hours ago ***NEWS***

Microsoft worked closely with US intelligence agencies to intercept users' communications, going as far as helping the NSA break the company's own encryptions.

SECURITY

The NSA/Prism firestorm: Will personal privacy become a thing of the past?

09 Jul 2013 ***FEATURES***

Given the Prism affair, the discussion about what's done with our personal data is one that we really shouldn't put off any longer.

SECURITY

Anonymous search engine DuckDuckGo sees surge in wake of Prism scandal

19 Jun 2013 ***NEWS***

Increasing numbers of Internet users are migrating to DuckDuckGo, as the NSA's web surveillance tactics scare people off using Google and Bing.

SECURITY

Prism: GCHQ 'penetrated BlackBerry security' to spy on G20 attendees

18 Jun 2013 ***NEWS***

The spying was carried out by GCHQ, the UK equivalent of the NSA, according to documents provided by Edward Snowden; Meanwhile Prism has been defended once again in the US.

SECURITY

Prism latest: Apple, Microsoft and Facebook reveal US government's data request figures

17 Jun 2013 ***NEWS***

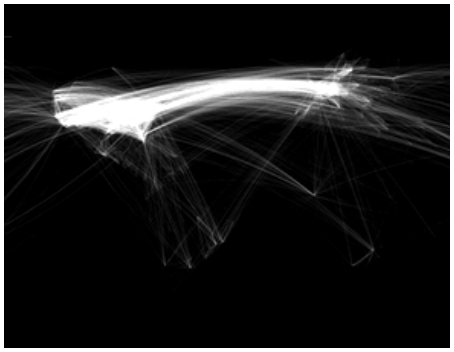
The fallout from Prism continues today as Apple joins fellow tech giants Microsoft and Facebook in revealing the amount of data requests it has received from the NSA.

SECURITY

Why the NSA's Prism leak could fundamentally alter or even break the Internet

11 Jun 2013 ***ANALYSIS***

The Prism leak which hit late last week is likely to have considerable long-term consequences for the entire Internet.



0 comments

★ 0

Leave a message...

Best Community Share

No one has commented yet.

Comment feed Subscribe via email