GRI + LEED - join us in las vegas **TWITTER TODAY -** SAP: millennial entrepreneurs **NEW SERIES -** GUIDE TO CARBON OFFSETS

« Back to Home Page

What Does Corporate Responsibility Mean When It Comes To NSA Data Requests?

Mary Mazzoni | Thursday July 31st, 2014 | 1 Comment

Read more in this series

Details about the National Security Agency's "Prism" surveillance program have entered the news in dribs and drabs since former NSA contractor Edward Snowden leaked revealing documents about the program to the Guardian and the Washington Post in June of last year. The unsettling insights revealed by Snowden generated quite a stir in the press, and large tech and telecom companies faced a wave of consumer backlash in the wake of the ongoing story.

Last September, while Snowden was living under guard at a secret location in Russia, Yahoo CEO Marissa Mayer seemed caught off-guard when a reporter raised questions about NSA surveillance at the 2013 TechCrunch Disrupt conference in San Francisco.

When asked what would happen if Yahoo ignored the order or shared it with the press, Mayer uncomfortably replied: "Releasing classified information is treason. It generally lands you incarcerated."

Companies are often left with few options once the U.S. government starts putting the screws to them. So, how do NSA data requests fit in with overall corporate responsibility? What is a company to do when faced with a request that seems to counteract its responsibility to consumers? We spoke with three key experts in corporate social responsibility (CSR) to find out the answers.

A few months before Mayer spoke at TechCrunch Disrupt, Yahoo, along with other tech giants like Google and Microsoft, asked a U.S. surveillance court to open up records that would allow companies to be more transparent, but the requests were denied. "Releasing information that could induce adversaries to shift communications platforms in order to avoid surveillance would cause serious harm to the national security interests of the United States," Department of Justice lawyers wrote in the redacted brief, issued on Sept. 30, 2013, as reported by PC World.

Predictably, companies, concerned citizens and privacy advocates were furious. But they got a bit of a reprieve in February, when the Obama administration agreed to relax some of the restrictions that barred companies from disclosing how many data requests they receive from the NSA. Under the new rules, a company can now report on how many requests for member data it has received, the number of accounts impacted and the percentage that they respond to. The rule came with some caveats: Although the aggregate data covers a six-month period, it can only be published six months *after* the reporting period has passed. The rules also prohibit young tech startups from disclosing data about NSA data requests for their first two years in operation.

« Series Main Menu
Click for main index

ABOUT THIS SERIES

The future of business lies within a wholly digital and connected world. Without the right systems in place to manage and protect the enterprise, however, businesses run the risk of overexposure and vulnerability for exploitation. This presents a new mantra: if it's connected, it must be protected. In this series, we will outline some of the data security challenges facing companies and showcase data protection as both a business and social imperative.

ABOUT SYMANTEC CORPORATION

Symantec

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Symantec considers the protection of information central to corporate responsibility in this digital age. Our innovative products and services protect people and information in any environment – making it possible for people to enjoy the full benefits of the connected world. We are based in California's Silicon Valley.

Symantec. Cyber Career Connection

Launched in June by Secretary Hillary Clinton at the 2014 Clinton Global Initiative America meeting, Symantec Cyber Career Connection (SC3) seeks to address the global workforce gap in cyber security and provide new career opportunities for young adults

Lawsuits from Google, Microsoft, Yahoo and Facebook were dropped as a result of the new rules, but companies were quick to note that further change was needed. “We filed our lawsuits because we believe that the public has a right to know about the volume and types of national security requests we receive,” a representative for Google, Microsoft, Yahoo and Facebook **told the New York Times** in a joint statement. “While this is a very positive step, we’ll continue to encourage Congress to take additional steps to address all of the reforms we believe are needed.”

Nancy Mancilla, founder and CEO of **ISOS Group** and a leading expert on CSR reporting also spoke in favor of further reform in a recent interview with Triple Pundit: “It’s ridiculous that for six months [companies] are quarantined before they can release that information. In this digital age, with companies that are in that space, it just doesn’t seem right.”

What’s a company to do?

Protesters gather in Washington, D.C. for the ‘Stop Watching Us’ rally in October 2013.

The **American Civil Liberties Union (ACLU)** has been particularly vocal in its stance against NSA spying, participating in several rallies in Washington including **Stop Watching Us** in October 2013 and **The Day We Fight Back** in February. A year after the story first hit the press, **the organization released a white paper** calling for further privacy reform.

Along with action points for Congress, the president and the courts, the ACLU provided five ways for tech companies to take action:

1. **Insist on warrants:** Surprisingly, warrants based on probable cause are not always a given when it comes to NSA data requests. In their call-to-action, the white paper’s authors note, “The fact that the government often withdraws requests when companies push back demonstrates just how out of control the government’s informal information-gathering has become.”
2. **Notify users of surveillance requests:** Companies are now permitted to disclose the number of data requests they receive, although with some limitations, yet many choose to remain silent, the ACLU notes.
3. **Minimize data collection and retention:** On the surface, this may seem a touch unreasonable, but the ACLU has no qualms with businesses holding onto data for as long as they need it for standard operating purposes, while noting, “Companies shouldn’t be holding onto our information without a truly valid business reason to do so.”
4. **Encrypt and protect our communications:** The ACLU suggests tech companies use encryption software like **STARTTLS** to protect email sent from one service (like Gmail) to another (like Hotmail).
5. **Publish meaningful statistics about government surveillance requests:** The authors note that “technology companies are the only ones who can give the public a full understanding of the way in which the government is using its various law-enforcement authorities to collect user data” and called for more reporting to the fullest extent the law allows.

Marc Gunther, veteran journalist, speaker and editor at large of **Guardian Sustainable Business U.S.** gave an additional suggestion to companies looking to spur change:

who may not be college-bound. In partnership with leading educational and workforce development non-profits YearUp and NPower, the program attracts, educates and trains underserved young adults (ages 18-29) to enter the exciting and in-demand field of cyber security.

MORE IN THIS SERIES:


Targeted Marketing and Online Privacy


Symantec Brings Cyber Security Jobs to HS Grads

Symantec Twitter Chat Recap: “Bridging the Workforce and Diversity Gaps”


Users Concerned About Data Security, Companies Slow to Respond

Small Business Survival: The Real Risks with Viral Success

Behind the Scenes: A Look at the Creation of Symantec’s Signature CSR Program


Why Insecure Data Is Bad for the U.S. Economy


Preparing the Next Generation for Ethical and Safe Online Engagement

What Does Corporate Responsibility Mean When It Comes To NSA Data Requests?

Storing Data in the Cloud: How Safe is It?


Can Companies Restore Consumer Confidence After a Data Breach?


Heartbleed Continues to Threaten Internet Security and Consumer Trust


Symantec Bets on Next Generation of Cyber Security Workers

> quote
>
> "The other thing that's incumbent upon them to do is to get active in the public policy arena," Gunther told Triple Pundit. "So if [companies] feel like there are either too many requests or if the requests aren't fully supported by evidence, they need to be very loud in Washington about trying to put some restrictions on the government's efforts to pry information out of them … Transparency — and noisy transparency — is a pretty good weapon."

Mancilla of ISOS Group agreed, saying "it's almost [a company's] duty" to get active around policy that impacts its users. That said, both experts agreed that being as transparent as possible under the law can do a great deal to ease users' minds and help companies recover from damage to their reputations. Elaine Cohen, CSR strategy expert and founder of **Beyond Business Ltd.**, a social and environmental business consulting firm, agreed, saying disclosing information about data requests is a "very powerful part of this dialogue."

The USA Freedom Act: A chance for reform

Introduced in October 2013 by a Democratic senator and a Republican House member, the **USA Freedom Act** seeks to significantly limit the collection and use of Americans' information under current spying laws. Rep. Jim Sensenbrenner (R-Wis.), a lead author of the **Patriot Act** and co-sponsor of the bill, had strong words for current data-gathering practices:

> quote
>
> "I authored the Patriot Act, and this is an abuse of that law," **Rep. Sensenbrenner told the ACLU**. "This misinterpretation of the law threatens our First, Second and Fourth Amendment rights. Congress never intended this. I will rein in the abuse of both the Patriot Act and the U.S. Constitution with the support of the American public."

Sen. Patrick Leahy (D-Vt.), chairman of the Senate Judiciary Committee and co-sponsor of the bill, echoed Sensenbrenner's sentiments, saying the "government has not made its case that this is an effective counterterrorism tool, especially in light of the intrusion on Americans' privacy rights."

Specifically, the bill would amend Section 215 of the Patriot Act – which is used to "collect the phone records of almost every American every day," as well as **gather Internet metadata en masse** – so that it can no longer be used in such a sweeping fashion, Michelle Richardson, legislative counsel for the ACLU's Washington Legislative Office, **said in a blog post** last fall.

A version of the bill was **passed by the House in May**, but some critics said "the bill's language governing data-gathering was ambiguous, raising concerns that it still would allow the large-scale collection of data from phone companies and other entities," **Ellen Nakashima of the Washington Post reported**. Senate aides **told the paper last week** that a compromise bill could be introduced in the Senate before the August recess.

"I don't even think this a CSR thing," Elaine Cohen said bluntly. "I think most people would agree that any en-masse infringement of privacy just doesn't make sense … Indiscriminate, unlimited exposure of potentially sensitive information shouldn't be the way governments do business."

The bottom line

A growing number of companies are pushing for change at the policy level, and the proposed Freedom Act would **create a panel of advocates from outside the government** allowing a wider section of stakeholders to weigh in. While it's disconcerting that NSA data requests to companies like Google have **increased by as much as 120 percent since 2009**, it may be time for users to start giving some of these tech companies a break.

"The first responsibility of any corporation is to obey the law," Cohen said. "And if the law says you must reveal certain aspects of your operations, which may include some of your customer data, then a company has every duty and responsibility to first and foremost comply with the law."

"Ultimately corporations have to do what they [can] to raise awareness for things that the law is demanding that may not be reasonable or that may not be in the public interest," she continued, "but … at the end of the day companies can't pick and choose which laws to obey."

Marc Gunther agreed, quoting what has now become a popular idiom — **if you're not paying for a service, you become the product** — and pointing to the now-commonplace practice of tech companies harvesting user data for advertising purposes.

"We, by the very nature of using a free service like Gmail, Facebook, Yahoo Mail, Twitter, etc., if we're not paying for it with dollars and cents we're in a sense paying for it by agreeing to be sold to advertisers," he told Triple Pundit. "So it shouldn't come as a shock that some of that information makes its way into the hands of the government."