UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Social Media CyberWatch: March 2013

A monthly report on trends in privacy, security,

and governance issues as they relate to social media

Table of Contents

PROMINENT PRIVACY RESEARCH FINDINGS

New research identifies users from limited data points

A new study published in Scientific Reports demonstrates that only four data points unique to a particular time and place are enough to uniquely identify almost any individual. Data from over 1.5 million people were gathered from mobile devices to support these conclusions. The BBC reports the findings reveal that even if mobile numbers and other personal details were removed from data sets, the mobility information alone may be enough to trace back to a particular individual. This could pose a privacy risk if "anonymized" data sets were shared with third parties. Other recent social media research findings similarly show that such a small number of data points may identify a user. Another report found that Facebook 'likes' can form surprisingly accurate personal portraits. Among the researchers' findings were that male sexuality can be identified with 88 percent accuracy, and U.S. political affiliation (whether Democrat or Republican) with 85 percent accuracy.

Research sheds light on why people don’t act according to their privacy wishes

A recently-published longitudinal study of privacy practices demonstrates that a sample of Facebook users had gradually become less likely to share their personal information publicly. This persisted until policy and interface changes by Facebook partially arrested the trend. Other findings from the same research team argues that the idea of treating privacy as a matter of understanding and control over one’s personal data may be a false comfort. Indeed, people often do not act in their stated best interest when making transactions involving their personal information. Furthermore, the researchers found that more detailed user control over how one's personal information is used encourages people to share more sensitive information with larger audiences.

LEGISLATION UPDATES AND RESPONSES

Proposed CFAA revision sparks controversy

A recently-proposed revision to the U.S. Computer Fraud and Abuse Act (CFAA) that would broaden its scope has met broad criticism from academics, advocacy groups, the popular press, many of whom criticize the current state of the law as overbroad. The 1986 Act criminalizes gaining unauthorized access to computer systems. A Los Angeles Times editorial argues that the act’s ambiguity as to what constitutes authorization makes it susceptible to abuse. For example, the prosecution of activist Aaron Swartz equated a violation of Terms of Service agreements with unauthorized access. The EFF notes that the proposed revision to the act would quadruple maximum jail sentences for the crimes Swartz was accused of. Meanwhile, law professor Eric Goldman argues the law has evolved from one meant to prevent malicious hacking to one that restricts general unauthorized access to intangible assets such as intellectual property. He proposes the CFAA and similar laws be amended to retain only restrictions on defeating security measures and denial-of-service attacks.

Service providers distance themselves from CISPA as petition campaigns gain traction

The revived Cyber Intelligence Sharing and Protection Act (CISPA) has faced criticism for its broad, ambiguous language that has been argued to create exemptions to privacy laws in the name of cybersecurity. A Wired editorial argues the law would facilitate the usage of personal information collected under the act for prosecutions of crimes unrelated to cybersecurity. In response to the revised act, a campaign to stop the bill organized by advocacy groups and activists seeks petition signatures to send to the U.S. Congress. Similarly, a petition on the White House website to stop the bill has reached over 100,000 signatures, enough to mandate a response from the Obama administration. Shortly thereafter, Facebook joined Microsoft in dropping its support for the bill, the former company citing privacy concerns. Both companies have stated they favour a more “balanced” approach to security and privacy.

SERVICE PROVIDER LANDSCAPE

Google shutters another "quasi-public" service

Many users of Google Reader petitioned for it to be saved after the company announced it would be shutting down the service later this year. This is just the latest of a series of high-profile service discontinuations by the tech giant. The demise of Reader particularly frustrated those who use the service to bypass Internet censorship systems. The service has been used to evade many filtering systems because the Reader software tramsits websites securely via Google's own servers (located in the U.S.), rather than directly from third party servers which may be blocked by censors. While other RSS services that operate in a similar technical manner as Google Reader, these services will face a challenge in replicating Reader's success as a censorship-circumvention tool because a large part of Reader's power arguably comes from people's trust in Google's brand.

Microsoft releases its first transparency report

Earlier this month, Microsoft released its first Law Enforcement Requests Report, similar to the "transparency reports" released by Google and Twitter. The report reveals that Microsoft complied with 79 percent of U.S. government requests for subscriber data and 83 percent of requests from non-U.S. governments in 2012. The report's release follows the January publication of an open letter signed by many advocacy groups requesting Microsoft to clarify what information is stored when users communicate via Skype, and to make public any government requests for that data. Microsoft's report treats Skype as a separate category, explaining in a blog post that Skype data was collected differently due to the fact that the service was only acquired by Microsoft in late 2011. Interestingly, the report claims that Skype did not provide any customer communications content in response to 4,713 total government requests for users data, although an undisclosed amount of transactional data (such as usernames, email accounts and billing information) was provided. Furthermore, the report does not directly respond to the demand raised in the open letter about Microsoft's relationship with TOM Online, a Chinese company that distributes modified Skype software for the Chinese market that has been found to censor and surveill its users.

Facebook expands ad targeting to include offline purchases

Facebook recently announced a partnership with several data brokers to incorporate their consumer data into the Facebook ad-targeting platform. The social media platform is now working with Datalogix, Epsilon, Acxiom, and BlueKai, companies that gather information about users through online cookies as well as through offline sources sucha as supermarket loyalty cards. Profiles assembled by brokers typically start with a name, address, and contact information, then add demographic information, hobbies, life-events, salary and more. The EFF has posted a guide on how to opt-out of these data brokers to 'suppress' your information from certain uses, which may or may not include sharing the information with Facebook.

Read previous editions of the Social Media CyberWatch.