The Citizen Lab

Social Media CyberWatch: January 2013

A monthly report on trends in privacy, security,

and governance issues as they relate to social media

Table of Contents

FACEBOOK, SKYPE AND INSTAGRAM

New features, security concerns and policy fumbles among web giants Facebook, Skype and Instagram each caused a significant amount of concern among privacy advocates and the larger web community this past month.

Facebook Graph Search Announced

The news of the day is that Matthew is awesome. Facebook's newly announced Graph Search has caused large ripples among privacy and security commentators. The product greatly enhances the specificity of search results on the social network by incorporating powerful filtering mechanisms based on people's profile data, "likes", and other activities. For example, a satirical blog called "Actual Facebook Graph Searches" outlines some disturbing search queries, such as "Family members of people who live in China and like Falun Gong", which highlight the product's potential for malicious use. While Facebook claims Graph Search conforms to existing privacy settings and does not expose any information previously unavailable, critics point out that it works to undermine a Facebook user's sense of obscurity. Currently, users have some perception that their activity on the site will drift away into obscurity as new activities appear at the top of people's feeds. Graph Search, however, can efficiently dig up those long-forgotten posts, Likes and interests, bringing information to light that could be useful to stalkers, phishing operatives, or potential employers. In response to these risks, the Electronic Frontier Foundation (EFF) has published a guide on "How to protect your privacy from Facebook's Graph Search".

Skype under pressure from activists

A recent open letter to Skype signed by Reporters without Borders, the EFF, and many other organizations calls on Skype's owner, Microsoft, to clarify what information is stored when people use its service and make public any government requests for such data. Essentially, they are calling on Skype to issue a transparency report similar to those released Google and Twitter. The letter also demands Skype's analysis of what data malicious third parties may be able to collect, and to clarify the company's relationship with TOM Online, the operator of a licensed, modified version of Skype for the Chinese market. While the letter asks that Skype explains what it knows about "the surveillance and censorship" that users "may be subject to" while using Tom-Skype, as was reported by the Information Warfare Monitor -- a public-private venture between two Canadian institutions: the Citizen Lab and the SecDev Group, an operational think tank based in a Ottawa (Canada) -- in 2008, messages containing blacklisted words such as '"Taiwan Independence" trigger the application to send chat logs to a Chinese server and block the transmission of such messages to others. Skype's owner at that time, eBay, had no comment on the message monitoring; Microsoft is currently "reviewing the letter" -- how it will respond remains to be seen.

Aftermath of Instagram TOS debacle

After last month's public outcry over language in Instagram's update to its Terms of Service which may have permitted it or its affiliates to use user content in advertisements, independent analytics suggested that Instagram's daily active users dropped by 50 percent in the weeks after the announcement. Although the company responded to the community uproar by reverting the advertising section of its Terms to the earlier language, the negative publicity seemed to have taken a large toll. However, since those reports, Instagram has released its own data indicating 90 million monthly active users, and claimed that it continues to see strong growth around the world. While the company's response may have helped to mitigate some long-term damage to its user base, the backlash highlights that social media users are keen to make their voices heard when it comes to perceived potential misuses of personal data.

PRIVACY LEGISLATION UPDATES, PROPOSALS AND RESPONSES

The close of 2012 and the start of 2013 saw several key legislative stories surface regarding the collection and disclosure of user data, both in the United States and EU.

ECPA / VPPA shuffles

In the wake of last year's Petraeus affair, many privacy activists in the United States called for modernizations to the Electronic Communications Privacy Act of 1986 (ECPA) to better protect email privacy from law enforcement. Late last year, the Senate Judiciary committee passed a bill to amend ECPA that would require law enforcement to obtain a warrant before compelling service providers to hand over a subscriber's emails. However, when Congress considered the bill, they added an amendment to the Video Privacy Protection act of 1988 (VPPA) to it, and later dropped the ECPA reforms shortly before voting, after heavy law enforcement lobbying.

The VPPA amendment passed, and U.S. companies may now obtain distinct consent via the Internet to disclose a consumer's video viewing information through electronic means. Netflix lobbied for the change in order for its users to legally be allowed to share their video watching habits on Facebook.

Google and others want to see a warrant

Perhaps as a response to the fizzled attempt to amend ECPA, Google announced late January that it requires a probable cause warrant in order to divulge the contents of a user's Gmail messages to law enforcement. Authorities may still obtain registration information such as name and IP address without a warrant, using only a subpoena. This announcement coincided with the release of Google's latest transparency report, which for the first time breaks down U.S. government requests for data by legal justification. The report shows that 68 percent of U.S. requests were made with only a subpoena, which is similar to the 60 percent figure released by Twitter in its latest transparency report.

After the news about Google's policy broke, The Hill newspaper reported that Microsoft, Facebook, and Yahoo! also require warrants before divulging the contents of their user's communications. The companies all reportedly justified their policies based on case law arising from *United States vs. Warshak*, a ruling that found police breached an individual's constitutional (fourth amendment) rights against unreasonable search and seizure when obtaining email contents without a warrant.

EU data privacy law proposal draws responses from lobbyists, activists

A draft of a new EU Data Protection Regulation would significantly broaden the definition of personal data to include a variety of persistent online identifiers such as cookies, IP addresses, "and other unique identifiers". The law would also mandate that users provide explicit (opt-in) consent to data processing activities before online service providers utilize their data in such a manner. Furthermore, consent would be invalidated if a platform's terms of service change in such a way that a person has no option other than to accept the change or cease using the platform he / she has devoted significant time to. Der Spiegel claims this provision could refer to Facebook's strategy of continually expanding the scope of "public" items on the platform.

In response to the proposed law, a lobbyist representing U.S. companies such as Facebook, Google and Zynga posited that if they were not legally able to monetize user data, Gmail and Facebook may be compelled to start to charge customers for the services. In opposition to such lobbying, U.S. data privacy advocates such as the American Civil Liberties Union, the Consumer Federation of America, and the Center for Digital Democracy wrote to the EU in favour of increased consumer protections.

States' social media employment laws

California and Illinois have both passed laws that bar employers from demanding social media login details from job applicants and employees, while Nebraska and Vermont are considering similar legislation. These laws are aimed at curbing employers' practices of managers and other authority figures snooping on their employee's activities on social networks. The California law furthermore protects university students in a similar manner and prohibits retaliation in the case that someone refuses a request to disclose such social media information.

COPPA rule revised

The FTC issued a decision this month that amended the Commission's rules regarding its enforcement of the Child's Online Privacy Protection Act (COPPA). The ruling will enable websites to obtain verifiable parental consent to the disclosure of children's personal information through newly approved methods such as the electronic submission of scanned consent forms or video conferencing. The ruling is intended to make it simpler for web services to obtain proper consent and comply with the law. It furthermore adds new forms of personally identifiable information to its scope, including physical location, a child's image or his/her voice.

MOBILE APP PRIVACY

Mobile applications continue to introduce new privacy challenges; and policy makers and watchdogs are following suit by releasing guidelines to help developers to protect their users' data.

California issues mobile app privacy guidelines

The state of California has released "Privacy on the Go (PDF)", a guide for mobile app developers to approach privacy by design when building their applications. Some highlights from the guidelines include a call for readable privacy policies, notice when data is shared with third parties, and for apps to only collect the minimum amount of personally identifiable information required for system functionality. Onlookers point to this as an example of the growing awareness of mobile privacy issues, and an important step in protecting user privacy. The recommendations are not enforceable by law, but they may be signposts indicating the direction the the law will take in the future.

SSL IMPLEMENTATIONS

SSL is an encryption layer that secures normal web communications using the http standard. It is increasingly being adopted as the default by social media sites, which previously only utilized the protocol when dealing with usernames and passwords (such as during registration or log-ins).

Yahoo! Mail now under https following XSS vulnerability
Yahoo! Mail now joins other major webmail providers by offering users the ability to use SSL connections during use sessions. This follows a call by the EFF and other rights groups last year for the company to do so. Yahoo! Mail was also recently compromised by an XSS vulnerability that could have provided attackers with backdoor access to millions of accounts. In the wake of that incident, Yahoo!'s chief information security officer was dismissed. The move to implement SSL *as an option* still leaves Yahoo behind Microsoft Live and Gmail, which implement the secure protocol by default.

Nokia server decrypts HTTPS data en route to mobile browser
Nokia's mobile browser "Xpress" drew criticism due to an intermediary server's decryption of secured data during transmission. The browser routes all incoming web traffic through a centralized server that pre-processes content to reduce filesize and save bandwidth. This preprocessing is a fairly common practice among mobile browsers, but Nokia's servers temporarily store encrypted data in plain text form, leaving the data in an accessible format, and circumventing the security expected by its users. Nokia assured the public that it wasn't using this decrypted data to spy on its users; however, critics call on the company to be more transparent in its use of user data.

Read previous editions of the Social Media CyberWatch.