Facebook fallout—Americans' privacy at risk across entire tech, information industry

March 23 2018, by Jennifer King

Credit: UC Berkeley

As fallout from the revelation of Cambridge Analytica's misuse of Facebook user information continues, many are mistakenly calling this incident a breach. Facebook is right to claim this incident was no breach

— this is Facebook's platform working exactly as designed.

I know, because I too created a survey app on Facebook for the express purpose of harvesting users' profile information. Except in my case, my academic research project was not engaged in deception and theft, and my co-authors and I used the data we gathered in part to understand both how much data we could obtain — legitimately — through the protocols made available to third-party app developers, and whether Facebook users understood what was occurring.

Facebook opened itself up to third-party developers back in 2007. Apps deployed on Facebook quickly became the rage, from Words with Friends to the many iterations of Farmville and the like.

There were no barriers to sign up as a Facebook developer; literally, anyone who could build an app could do it. Much like any online sign-up process, one needed only to agree to the site's developer terms and conditions and have enough technical proficiency to deploy an app. If you could convince other Facebook users to "install" it on their profiles, as a developer you were instantly rewarded with a trove of data that exceeded what was available on a user's profile.

My colleagues and I did this in 2010, creating an app we called "What kind of Facebook user are you?" In our project approved by UC Berkeley's Institutional Review Board, we conducted a survey where we asked Facebook users questions about how third-party apps worked, the types of data apps could access from their profiles, and their privacy concerns. We published our findings in 2011.

'An incident like this was inevitable'

The process for launching the app was trivial and provided us with not only with the user's data, but also a smaller set of data from their entire

social graph: all of their Facebook friends. It is this feature of the API (now discontinued) that allowed Cambridge researcher Dr. Aleksandr Kogan to vastly expand his dataset past the few hundred thousand who actually responded to his survey. For example, our 516 respondents had over 129,000 friends, whose basic profile information we also could have gathered.

Many of us in the privacy research community were aghast at the Facebook API's leniency when it launched, and speculated that an incident like this was inevitable. As researchers who focus on privacy and social media, we wanted to understand whether Facebook users understood exactly what was happening when they elected to add an app to their profile. At the time we conducted our survey, about half of our respondents did not know that apps could access and store their profile data off of Facebook's site, or that when they added an app, it could also access the basic profile data of anyone on their friends list.

Further, we asked specifically about the kinds of practices Cambridge Analytica engaged in: over 90 percent of our respondents were somewhat or very uncomfortable with the possibility that an app could sell their profile information, store their information permanently on its own servers, or share that data with other companies.

The Facebook Platform API was notable for its obvious lack of concern for users' data. Although the company eventually limited access to some profile data and removed the open access to the users' social graphs, Facebook did not screen its third-party developers (and still does not). As this incident shows, the company cannot meaningfully police its developers. When one considers the substantial number of third-party apps offered across their platform, there is no practical way Facebook can ensure that there aren't hundreds — or even thousands — of additional Cambridge Analyticas lurking out there and engaging in similar behavior.

Herein lies the conflict: the companies that traffic in user data in the United States have worked hard to fight any legislative oversight. Instead, they promise to self-regulate, yet as this incident demonstrates, we can't trust them to enforce the terms of their own business agreements. To be fair, this problem is not limited to Facebook; a lack of oversight has repeatedly put Americans' privacy at risk across the entire technology and information industry. Congress has repeatedly failed to pass legislation protecting Americans from the most egregious information collection practices.

Since we can't rely on Congress to act, at a minimum Facebook should either discontinue or drastically alter its developer program to ensure that only a bare minimum of user profile data is ever shared outside the company. Further, the company should engage in active oversight of any third parties that have access to its users' data to ensure that anyone who seeks to engage with its users does so with benign intentions. Given that we've already seen how poorly the company has supervised its advertising sales operations, I'm pessimistic they can accomplish this feat.

In its effort to quickly dominate the social networking landscape, Facebook put growth ahead of its users. Now that the inevitable has occurred, we see that it wasn't just Facebook users who were put in jeopardy. Rather, the health and future of our democracy is at stake.

More information: Privacy: Is There An App For That? www.jenking.net/pubs/privacy-i … ere-an-app-for-that/ Jennifer King et al. Privacy, *Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11* (2011). DOI: 10.1145/2078827.2078843

Provided by University of California