United States: Far-right “researchers” steal Facebook info

Tuesday 24 April 2018, by SOLENBERGER Peter (Date first published: 14 April 2018).

On April 9 Facebook began notifying 87 million users that Cambridge Analytica, a far-right political consulting firm, had accessed their information, including their private profiles, postings, likes and friends. Facebook claims that in April 2015 it blocked the path by which Cambridge Analytica accessed the data, but it didn’t acknowledge the massive breach or suspend Cambridge Analytica until now.

Contents

Other paths remain. On April 4 Facebook acknowledged that data-mining outfits may have used its search feature to access the public profiles of all two billion Facebook users, including whatever information they had neglected to make private.

The villains

Cambridge Analytica was started in 2013 by Steve Bannon and Robert Mercer to promote their shared agenda of robber baron capitalism, anglo-aryan nationalism and militarism. Bannon led the alt-right Breitbart News and was CEO of Donald Trump’s 2016 presidential campaign. He was Trump’s chief political strategist from the election until the two had a falling out in August 2017. Mercer is a hedge-fund billionaire.

Cambridge Analytica is an offshoot of the SCL Group, another Britain-based company, involved in military disinformation campaigns and attempts to swing elections around the world. Cambridge Analytica is SCL’s US affiliate.

In the 2014 US election cycle Cambridge Analytica was involved in 44 races, working with the John Bolton Super PAC to swing elections in North Carolina, Arkansas and New Hampshire. They helped Thom Tillis oust Senator Kay Hagan in North Carolina and helped Tom Cotton win a Senate seat in Arkansas. Their candidate Scott Brown lost his bid in New Hampshire. Bolton is now Trump’s National Security Advisor.

In the 2016 US election cycle Cambridge Analytica worked first for Ted Cruz, Mercer’s favorite, and then for Trump. In 2016 it also worked for the Brexit campaign.

Whistle-blower Christopher Wylie, a repentant cofounder of Cambridge Analytica, revealed that Palantir Technologies proposed the method by which Cambridge Analytica accessed the Facebook data.

Palantir analyzes data for US spy agencies, the Defense Department, local governments, hedge funds, banks and health insurance companies. Its largest shareholder is Peter Thiel, another rightwing billionaire. Thiel cofounded PayPal and was an early investor in Facebook. In 2016 he supported Trump and helped Hulk Hogan bring down Gawker Media.

The method

The method Palantir proposed and Cambridge Analytica used was quite simple. Cambridge Analytica hired Aleksandr Kogan and his company Global Science Research to conduct a phony personality quiz as a cover for acquiring Facebook data. Kogan is a Moldova-born lecturer in psychology at Cambridge University.

Whistle-blower Christopher Wylie testifies to British MPs
Kogan developed a Facebook app called "This Is Your Digital Life" to access the data. He recruited respondents using Amazon's Mechanical Turk, an online employment bulletin board for tech-related tasks. Kogan promised respondents $1-2 dollars when they completed a brief survey. Utah-based Qualtrics ran the survey.

At the end of the survey respondents were directed to log in to their Facebook accounts so that the app could access their profiles. Buried in the fine print was a notice that the app would also access the data of all their friends, something Facebook allowed at the time.

Around 300,000 people took the survey and handed over their Facebook data and that of their friends. They had given their time and wanted their money. Most failed to read the fine print. A few respondents complained to Amazon, whose policies forbid Mechanical Turk employers to require workers to provide their personal information. Like Facebook, Amazon belatedly closed the barn door.

When Cambridge Analytica hauled in its net, it had data from 87 million people.

No surprise

The Cambridge Analytica ripoff of Facebook data should be no surprise. Mark Zuckerberg and his roommates began what became Facebook in 2004 as a website where Harvard undergraduates could post pictures of themselves and others and rate them as to who is hot and who is not.

Facebook has grown enormously since Zuckerberg's undergraduate days and now has more than two billion users. It's still used for ugly purposes and invites users to waste huge amounts of time. But it has also helped users keep track of family and friends and reconnect with people from their past. It has helped activists organize demonstrations and strikes and promote progressive political views.

Facebook isn't in business to help people communicate, however. It's in business to make money. Its business model is simple: Users give information to Facebook, and Facebook packages the information and sells it.

Facebook is phenomenally profitable. In 2017 its revenue was $40.653 billion, and its after-tax profit was $15.934 billion. Much of its revenue comes from targeted advertising. Some comes from selling tabulations of data supposedly aggregated enough to prevent identification of individuals.

Some comes from giving access to individual data through apps. The app owner, Cambridge Analytica in this case, pays Facebook to make the app available to users. When users access the app, it has access to their personal information and, at the time of the Cambridge Analytica theft, that of their friends.

The rationale is that the app provider can "enhance the app experience" with information about the app user. In the Cambridge Analytica case there was no "app experience," since the app's sole function was to access the Facebook data of users and their friends. The phony survey was conducted outside Facebook.

Targeted advertising is annoying and reminds us how much information Facebook and other social media have about us and can sell. The supposedly anonymized data tabulations are dangerous. The police or rightwing groups don't need individual data to learn when and where a demonstration or meeting will be. Facebook buzz about an event is sufficient. And tabulated data can often be combined with other sources of information to identify individuals.

Even more dangerous is the sale of individually identifiable information, such as the Cambridge Analytica data. It could be used to identify likely supporters of rightwing causes and candidates to turn them out in elections. But it could also be used to identify activists and dox (publicly identify) them for firing, harassment or violence.

In testimony to Congress on April 10 and 11 Zuckerberg expressed regret at the Cambridge Analytica leak but basically said that users who wanted to share information with others — the sole purpose of social media — had to accept that their information would be used however Facebook chose to use it. Their privacy settings apply only to other Facebook users, not to Facebook itself. Take it or leave it.

Lessons

At the individual level, the main lesson is to protect yourself as well as you can from the corporations which control the means of communication you use. Going beyond that, you can promote non-capitalist Internet alternatives now. Pretty much anything you can do with Facebook, Google and other capitalist data thieves you can do other ways. The box below has some suggestions.

At the political level, privacy reforms are much needed. Here are some obvious points for legislation: 1) Users should be told in clear language how the provider means to use their data, so that they can give or withhold consent. 2) No data should be mined or shared without their explicit consent. 3) The default should be that they opt out, not opt in. 4) People should have the right to be forgotten, with all their social media data scrubbed.

The right to privacy should be rigorously enforced. The social media corporations will try to evade the regulations, since their fabulous profits come from the misappropriation of data. The Internet billionaires need to know that violations will lead to the confiscation of their fortunes and years in prison.

In a socialist world electronic communication would be organized very differently. Social media platforms would be developed to serve the human need to communicate, not to make money for

billionaires.

No advertising. Data mining with informed consent for medical research and other scientific purposes, not data theft for profit. Open source. No patents or copyrights. Information should not be a commodity. To guarantee privacy, end-to-end encryption as easily available to ordinary folk as it is now to corporate executives.

There might still be problems with nasty comments, flame wars, device addiction, and so on. But free people would figure out how to deal with these.

Protect yourself on the Internet

With Facebook and other social media, consider whether you really need them. If you do, consider how much information you want to give them. Check your privacy settings. Who do you want to know what? Prospective employers check social media.

Keep in mind that there are many ways your information might get out. You or someone else might make a mistake with security settings. Facebook might carelessly expose your data. Hackers might break into Facebook servers. The government might obtain your data with a judicial warrant or a national security exception.

Remember that there's no "free" provision of Internet services. If you use unpaid Gmail, Google Groups, Google Docs or Google Drive, the arrangement is like that with Facebook: You provide the data, and they mine and sell it.

You have more protection with Internet services you pay for, since you and the provider have a contract which in theory you could enforce. But if you're corresponding with users of unpaid services or using unpaid email groups or collaboration tools, your contributions are being mined and sold too. Hacking and government interception are also possible.

The best security would be to use only encrypted email and messaging (Enigmail, Signal, etc.) and visit the Web only via secure connections (HTTPS) or Tor or other dark web networks. This is too cumbersome for most people. We each have to work out our own compromise between security and convenience.

Promote non-capitalist Internet alternatives

Thousands of tech experts have resisted being drawn into the orbits of Amazon, Apple, Facebook, Google, Microsoft, etc., and have developed Internet alternatives designed to protect users' privacy and promote open communication outside corporate control. Volunteer labor, individual donations, foundation grants, and fees for advanced services support this activity.

Linux, the most-used operating system for servers and supercomputers, and Wikipedia, the most-used reference source on the Internet, are examples. But pretty much anything you can do with a for-profit provider you can also do with a nonprofit provider.

Often the nonprofit alternative is somewhat more "geeky" and harder to use than its for-profit equivalent. The corporations generally have far more money for software development, they focus on their user interface, and they rely on their market share and familiarity to keep users.

Choosing an alternative provider is something like choosing a food co-op, farmers market or community-supported agriculture (CSA) over Kroger or Whole (Amazon) Foods. Less convenient, perhaps, but often a better product and the sense of contributing to a better world. Like other forms of pre-figuration, it won't displace capitalism, but it shows what might be done without it.

Here's a table of some common Internet services and movement or nonprofit alternatives to the capitalist providers. The table is not exhaustive. It's meant to indicate that there are alternatives, not to advocate any particular way to go.

Function Nonprofit alternative

Browser Firefox

Contact relations CiviCRM

Email Your Internet host, Riseup

Email client Thunderbird

Email lists Mailman with your Internet host, Riseup

Encrypted communication Signal, Enigmail

Internet host Koumbit, MayFirst

Microblogging Mastadon

Operating system Linux

Search engine DuckDuckGo

Team sharing Mattermost, Riseup Pad

Website Drupal, Joomla, Wordpress

Wordprocessing, spreadsheet, etc. OpenOffice

Organizers can't avoid Facebook, Twitter and other corporate social media, since our goal is to reach people, and for now they're on corporate social media. But as with newspapers, radio, television and other now-traditional media, we should balance access with security in deciding who is to do what.

Peter Solenberger

P.S.

* April 14, 2018:
http://www.solidarity-us.org/site/node/5292

* Peter Solenberger is a Solidarity member, activist and tech worker in northern Michigan.