

A developer created a script that updates your Facebook posts with gobbledygook.

Always ‘poison’ your social media data before you delete Facebook or Google

Christina Bonnington—M

Blind Survey: 31% of Tech Workers Will Delete Facebook Accounts Following Data Scandal (sludgefeed.com)

submitted 23 hours ago

by [Thomas_Crown](#) to **technology** (+32|-1)

10 comments

Two-Faced Facebook Says Connecting People is Worth More than Human Life While Actively Censoring and Disconnecting Conservatives (archive.is)

submitted 18 hours ago by [x0byte](#) to **news** (+100|-2)

7 comments



Over the past few weeks, we've learned a lot about Facebook, Cambridge Analytica, and how Facebook uses your data. The revelations have pushed many users—including some brands and celebrities—to leave the social network altogether. Rather than simply deleting your profile or profile information, however, some are advising a slightly different tactic to protect your online identity: tainting that data.

Developer and former systems administrator Kevin Matthew published a script that goes back through your Facebook posts and edits them with randomly generated characters.

Based on his knowledge as a systems administrator, Matthew explains that “even by conservative assumptions, your data never really disappears permanently” when you deactivate or delete your Facebook account. With that in mind, the next best thing, he argues, is to go back through your history on the social network and

“poison” (or otherwise obfuscate) all that data.

Matthew wrote a CasperJS script that does just that, automatically editing past posts with either random or pseudo-random letters. For this technique to be most effective, you wouldn't do it just once. Mathew proposes editing all of your Facebook data with this script roughly five times over a three-month period so your original data is sufficiently scrubbed from Facebook's multiple, redundant backup systems.

Mathew details his full reasoning, the technique, and how the script (which is really just a proof of concept) works in a blog post. It's possible that the script could be a violation of Facebook's terms of service, since it could be considered to impair or disable the proper functionality of Facebook. If you decide to give it a shot, keep that in mind.

In an interview with *Vice's* Motherboard, Mathew says that his main goal in creating the script isn't necessarily for it to make a huge impact among Facebook users, but rather to draw attention to the lack of

“right to be forgotten” laws in North America. Since the passing of such laws in Europe, Google has fielded more than 2.4 million requests to remove URLs from its search engine to protect peoples’ privacy.

In the U.S., we have no such laws. If Facebook or other social aggregators sell or collect your data, you typically have no legal recourse for getting it removed.

H/T Motherboard

The CLOUD Act, which was included in last week’s Omnibus bill, eviscerates what may have been left of citizen privacy in America and it makes personal information readily available to other governments. Foreign police now can wiretap communications from U.S. companies without a warrant, foreign nations can demand personal data stored in the US, the US president can make agreements to allow police in foreign nations to seize data in the US while ignoring US privacy laws, foreign police can obtain data without notifying the US government, and it empowers US police to grab any data from anyone, regardless of where it is stored. In other words, It empowers the US government and foreign governments to invade the privacy of anyone it wants to stalk. [The big question is why did President Trump sign such a bill when he could have vetoed it? The

assertion that Hillary would have been worse is not an answer to that question.] -GEG

While the nation remained fixated on gun control and Facebook's violative practices last week, **the U.S. government quietly codified the CLOUD Act, its own intrusive policies on citizens' data.**

While the massive, \$1.2 trillion omnibus spending bill passed Friday received widespread media attention, the CLOUD Act — which lawmakers snuck into the end of the 2,300-page bill — was hardly addressed.

*The **Clarifying Lawful Overseas Use of Data***

***Act** (CLOUD) “updates the rules for criminal investigators who want to see emails, documents and other communications stored on the internet,” CNET **reported**. “Now law enforcement won’t be blocked from accessing someone’s Outlook account, for example, just because Microsoft happens to store the user’s email **on servers in Ireland**.”*

The CLOUD Act will also allow the U.S. to enter into agreements that allow the transfer of private data from domestic servers to investigators in other countries on a case-by-case basis, further globalizing the ever-encroaching surveillance state. The Electronic Frontier Foundation, which has strongly opposed the legislation, **listed** several consequences of the bill, which it called “**far-reaching**” and “**privacy-upending**”:

- *Enable foreign police to collect and wiretap people’s communications from U.S. companies, without obtaining a*

U.S. warrant.

- *Allow foreign nations to demand personal data stored in the United States, without prior review by a judge.*
- *Allow the U.S. president to enter “executive agreements” that empower police in foreign nations that have weaker privacy laws than the United States to seize data in the United States while ignoring U.S. privacy laws.*
- *Allow foreign police to collect someone’s data without notifying them about it.*
- *Empower U.S. police to grab any data, regardless if it’s a U.S. person’s or not, no matter where it is stored.*

The bill is an update to the current MLAT (Mutual Legal Assistance Treaty), the current framework for sharing internet user data between countries, which both legislators and tech companies have criticized as inefficient.

*Some tech companies, like Microsoft, have **endorsed** the new CLOUD policy. Brad Smith, the company’s president and chief legal officer, called it “a strong statute and a good compromise,” that “gives tech companies like Microsoft the ability to stand up for the privacy rights of our customers around the world.”*

They echoed the sentiment of lawmakers like Orrin Hatch (R-UT). In February, he **said** of the bill:

“The CLOUD Act bridges the divide that sometimes exists between law enforcement and the tech sector by giving law enforcement the tools it needs to access data throughout the world while at the same time creating a

commonsense framework to encourage international cooperation to resolve conflicts of law.”

But one of the biggest complaints from privacy advocates, however, is that the new legislation places too much unmitigated power in the hands of governments with abysmal human rights records while also giving too much discretion to the U.S. government’s executive branch. **Noting that the executive branch will decide which countries are human rights compliant and that those countries will then be able to [engage](#) in data collection and wiretaps without any further restrictions or oversight**

[Read full article here...](#)