POLITICO

-Q-

Swedish Minister for Home Affairs Anders Ygeman gives an interview after resigning his position | Ari Luostarinen/AFP via Getty Images

Swedish ministers resign amid data security breach scandal

Citizens' sensitive personal information may have been leaked.

By **MARK SCOTT AND CONNOR MURPHY** | 7/27/17, 6:21 PM CET | Updated 1/28/18, 10:21 PM CET

Two senior Swedish ministers resigned on Thursday as the country's government tried to limit the political fallout from a security breach that may have led to large-scale disclosure of citizens' sensitive personal information.

Sensitive data was potentially leaked to contractors in Romania and the Czech Republic, among other Eastern European countries, who were employed to work on a project outsourced to IBM Sweden. The data breach — one of the largest in the country's history — included the potential disclosure of Swedish driving license records and classified information such as data on military vehicles.

While the extent of the leak remains unclear, it comes as governments worldwide are facing an increase in cybersecurity threats from groups of hackers, as well as those sponsored by other countries' intelligence agencies. There has been a raft of recent attacks around the globe as cyberattackers have targeted the British health system, Ukrainian banks and government agencies, as well as individuals from the United States to France.

The most recent leak in Sweden is not connected to such activities. But the accidental disclosure of masses of sensitive information on Swedish citizens, experts warn, highlights how policymakers often fail to implement the most basic protections to ensure citizens' digital data is kept safe.

> “I have to take responsibility for the country. It wouldn't serve Sweden to throw the country into a political crisis" — *Prime Minister Stefan Löfven*

Swedish Prime Minister Stefan Löfven said that Anders Ygeman, the country's home affairs minister, and Anna Johansson, the infrastructure minister, had both resigned because of the scandal. The prime minister refused to call an early election, despite demands from opposition political parties.

“I have to take responsibility for the country," he said on Thursday. "It wouldn't serve Sweden to throw the country into a political crisis."

The country's center-left government has been engulfed in crisis in recent days over a data security breach at the Swedish Transport Agency.

The resignations of two of the country's ministers shows how issues concerning individuals' privacy are quickly becoming hot-button topics in an ever-more connected world.

Privacy Settings

"There are national security and personal privacy implications to this data breach," said Simone Fischer-Hübner, a privacy and security professor at Karlstad University in Sweden. "There's been a lot of bad practices."

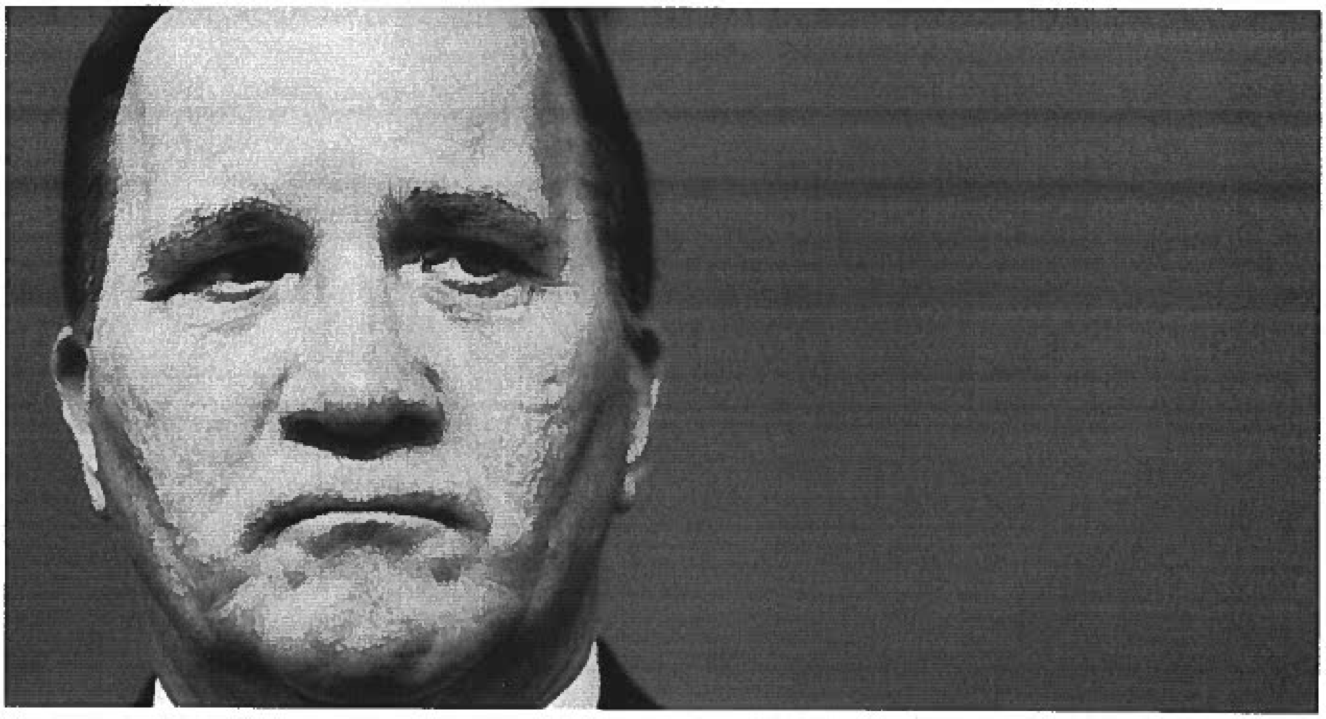
The controversy in Sweden dates back to 2015, when the country's transport agency outsourced its IT operations to IBM Sweden. Revelations about how the sensitive data was sent overseas and may have been illegally accessed by contractors was first made public earlier this month after local media reports claimed that Maria Ågren, the Swedish Transport Agency's director general, was fired and fined by the country's authorities in January for the mishandling of classified material.

The Swedish government said the damage from the data breach may have been limited, though Prime Minister Löfven confirmed that he was first informed about the incident in early 2017.

Earlier this week, Löfven, who is the leader of the Social Democratic Party, said the breach was "a mess" and had "exposed both Sweden and the Swedes to risks."

Nevertheless, Jonas Bjelfvenstam, the current director general of the Swedish Transport Agency, said there were "no indications that data was disseminated improperly."

IBM said that it took "data privacy very seriously," but would not comment further on the depth of the data breach.



Privacy Settings

Swedish Prime Minister Stefan Löfven speaks at a press conference | Jonathan Nackstrand/AFP via Getty Images

While two Swedish ministers have resigned over the scandal, a third — Defense Minister Peter Hultqvist — will remain in his post, despite opposition demands for his removal.

Sweden's opposition political parties have already called for a vote of no-confidence to unseat the government ministers caught up in the scandal.

"The first question I would ask is whether the Swedish Transport Agency, by outsourcing some work to what I presume are IT body shops in Serbia and the Czech Republic, simply granted those folks open access to its network," said Rik Turner an infrastructure analyst at Ovum, the technology research company. "If that is the case, then this was just plain stupidity."

Laurens Cerulus and Christian Krug contributed to this report.

Privacy Settings

CRISIS COMMUNICATIONS

Facebook, Amazon under a cloud of criticism over latest data leak

A security firm found millions of vulnerable Facebook records on an Amazon cloud server, raising new questions about users' safety and the social network's ties to third-party vendors.

By Ted Kitterman
@tedkitkat

April 5, 2019

LinkedIn Twitter Facebook

Pinterest Plus d'options... 9

Facebook has stepped into another steaming data scandal.

The social media platform can't seem to dislodge itself from the hot PR mess stemming from investigations into Cambridge Analytica and other third-party apps with access to users' information.

The company has tried op-eds from leaders Mark Zuckerberg and Sheryl Sandberg, blog posts and social media messages, a couple of media apology tours and, most recently, a high-profile call for privacy and regulation.

Throw another log onto the PR conflagration.

New reports suggest that third-party apps with prior access to user data were not held to adequate security standards, and Facebook will face additional scrutiny over exposed data.

*The Next Web*wrote:

> Flip that board that says "It's been _ days since we found a massive pile of unsecured Facebook data" right back to zero, and get ready to reset your passwords *again* just to be safe. Security researchers discovered hundreds of millions of records on publicly-accessible Amazon cloud servers — including names, passwords, comments, likes, and all the other stuff we should all just assume has already leaked at some point.
>
> Cybersecurity firm Upguard released its findings earlier today. There are two data sets, originating from different sources, both stored in Amazon S3 buckets — no password protection on either one, naturally. They've since been taken down.
>
> In this case, it's not Facebook itself holding the leaky bucket. The data originated from third-party sources, namely a media company called Cultura Colectiva and an app titled "At the Pool." The former is the larger of the two — according to Upguard, it includes 540 million records on user likes, comments, IDs and more. The latter apparently includes 22,000 Facebook passwords and email addresses.

[RELATED: Earn recognition for your incredible comms efforts**]**

Facebook doesn't have anything new to say about these latest reports.

The Next Web continues:

> A Facebook spokesperson told TNW, "Once alerted to the issue, we worked with Amazon to take down the databases. We are committed to working with the developers on our platform to protect people's data."
>
> Why does that sound familiar? Oh yeah…
>
> - "…we're making real progress and *we are committed*to continuing to improve." — *Expanding Our Efforts to Protect Elections in 2019*
> - "A lot of this work is in the early stages, and *we are committed*to consulting with experts, advocates, industry partners, and governments — including law enforcement and regulators — around the world to get these decisions right." — Mark Zuckerberg's *A Privacy-Focused Vision for Social Networking*
> - "But we are committed to getting it right so Facebook is a safe place for people and their friends." — *Working to Keep Facebook Safe*
>
> Facebook's major defense post-Cambridge Analytica was that it was limiting third-party apps' access to this very kind of data. But "At the pool," which was last used in 2014, apparently predates that measure. Upguard warned Facebook's previous privacy gaffes would continue to echo for all of us: "But as these exposures show, the data genie cannot be put back in the bottle."

Facebook wasn't the only company implicated; security researchers reported difficulty in getting host company Amazon to remove the compromised files.

*Bloomberg*reported:

> After security researcher Chris Vickery discovered millions of records from Facebook Inc. users sitting unsecured on a public database, he tried for weeks to get Amazon.com Inc., owner of the servers where the data were stored, to take it down.
>
> “We’re looking into the situation and assessing any extra steps we can take,” came the response from Amazon security staff on Feb. 21 — three weeks after Vickery initially brought the data exposure to Amazon's attention.
>
> The trove in question included 540 million pieces of information, such as identification numbers, comments, reactions and account names, that had been culled from Facebook pages and stored on Amazon servers by Mexico City-based digital platform Cultura Colectiva. The records were accessible and downloadable for anyone who could find them online, and they didn't get taken down until April 3, after Facebook — alerted by Bloomberg News — contacted Amazon.

The incident also raises questions of about who is responsible for data security when the data is stored in the cloud by providers like Amazon or Microsoft.

Bloomberg continued:

> AWS customers “own and fully control their data,” Amazon said in a statement. “When we receive an abuse report concerning content that is not clearly illegal or otherwise prohibited, we notify the customer in question and ask that they take appropriate action, which is what happened here.”
>
> Amazon has grown into the world’s biggest provider of on-demand data storage and computing power in part by pledging to big companies that their data will be as private in the cloud as it was sitting in a back-room server.
>
> “They just don’t want to start a precedent of them meddling with the data,” Vickery said, back when he was having trouble getting Amazon to take it down. “If they start shutting down access to data breaches, they start getting into liability a bit more. They’re in a sticky situation.”

Syracuse.com wrote:

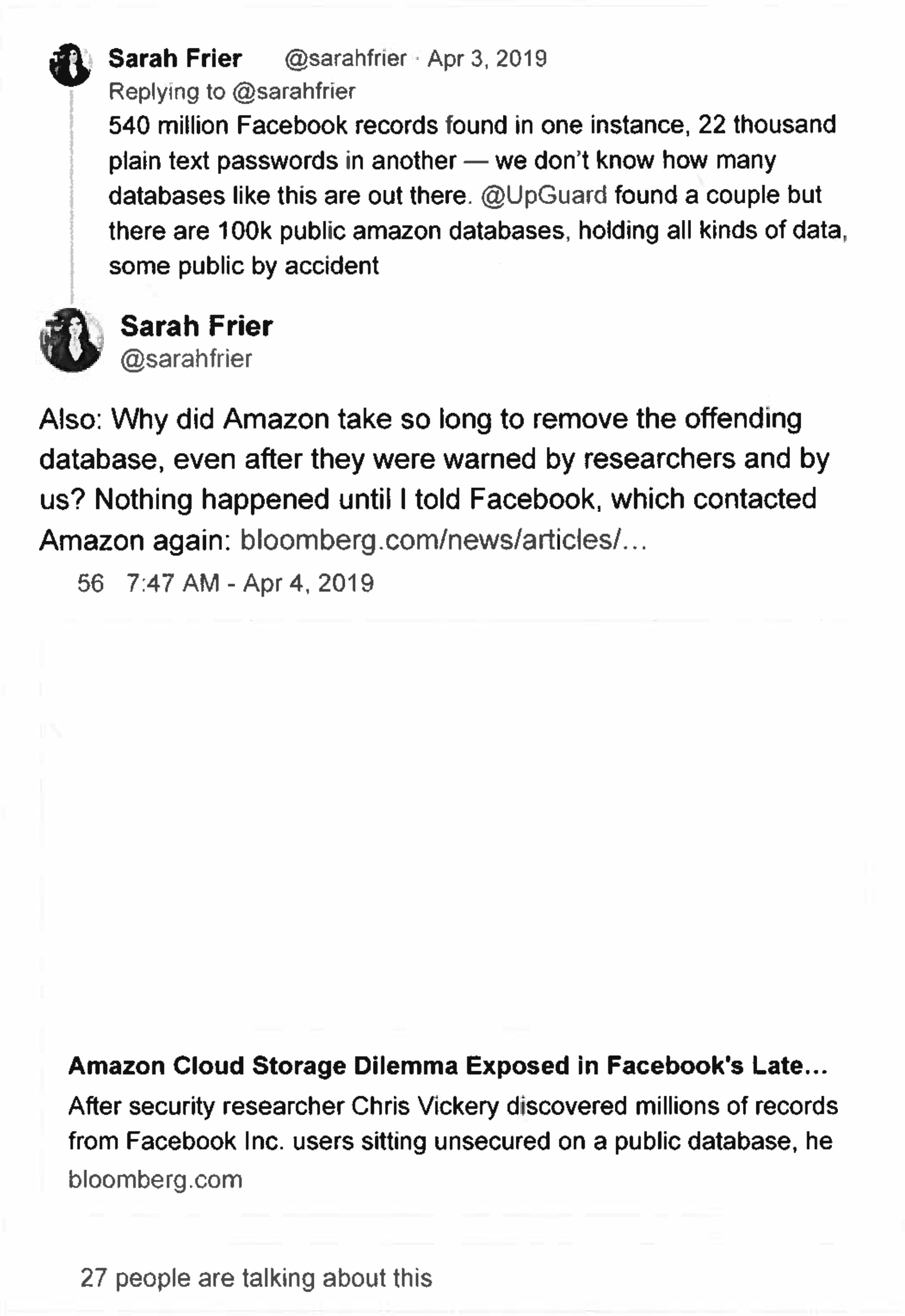
> "We are committed to working with the developers on our platform to protect people's data," Facebook said.
>
> But the fact that such a vast, full cache of sensitive personal information could have been accessed by anyone online raises fresh questions about Facebook's efforts to protect its users' privacy. The report from UpGuard comes almost a year after revelations that Cambridge Analytica, a political consultancy, improperly accessed the personal data of 87 million Facebook users with the aid of a quiz app.
>
> The exposure of Facebook's data also illustrated a hard reality: Once accessed or obtained, personal data can live forever.
>
> "All of the data passed from Facebook to literally millions of developers needs to be managed," said Greg Pollock, a vice president at UpGuard. "I don't know that Facebook can clean up the mess they've made. It's an oil spill – that data is out there."
>
> The first set of records appear to belong to a Mexican media company, Cultura Colectiva, which improperly stored data about people's friends, likes, photos, music, location check-ins and groups on a public Amazon server. Pollock said that UpGuard in January tried to notify the organization that its cache of Facebook information had been left open for anyone to download but ultimately received no reply.

On social media, some bemoaned the lag in taking down the compromised data:

Fercan Yalinkilic
@FercanY

It took weeks for #Amazon to take down 540 million Facebook info on the cloud accessible by everyone.bloomberg.com/news/articles/…

2 3:17 AM - Apr 4, 2019



Sarah Frier @sarahfrier · Apr 3, 2019
Replying to @sarahfrier
540 million Facebook records found in one instance, 22 thousand plain text passwords in another — we don't know how many databases like this are out there. @UpGuard found a couple but there are 100k public amazon databases, holding all kinds of data, some public by accident

Sarah Frier
@sarahfrier

Also: Why did Amazon take so long to remove the offending database, even after they were warned by researchers and by us? Nothing happened until I told Facebook, which contacted Amazon again: bloomberg.com/news/articles/…

56 7:47 AM - Apr 4, 2019

Amazon Cloud Storage Dilemma Exposed in Facebook's Late…
After security researcher Chris Vickery discovered millions of records from Facebook Inc. users sitting unsecured on a public database, he
bloomberg.com

27 people are talking about this

Both Amazon and Facebook have refrained from addressing this new report directly, instead pointing to overarching policy and efforts to educate the public about data security.

Reuters reported:

> “Facebook’s policies prohibit storing Facebook information in a public database,” the company said.
>
> Facebook has been hit by a number of privacy-related issues, including a glitch that exposed passwords of millions of users stored in readable format within its internal systems to its employees.
>
> Last year, the company came under fire following revelations that Cambridge Analytica obtained personal data of millions of people’s Facebook profiles without their consent.
>
> Facebook later announced changes aimed at protecting user data, including an audit of at least thousands of apps that have the right to access Facebook user data.
>
> Amazon did not respond to requests for comment. It has increased efforts to educate customers about the risks associated with storing user data publicly after several such data privacy lapses by its customers made headlines in recent years.

What do you think of the companies’ responses, *PR Daily*readers?

(Image via)

TOPICS: CRISIS COMMUNICATIONS

COMMENT

Name

Mail (will not be published)

Website

Enter your comment...

SUBMIT

PITCH US

RECOMMENDED READING

CONFERENCE ALERT

PR Daily Staff

3 ways to help your executives thrive in the digital world

WEEKLY ROUNDUP

PR Daily Staff

The 5 most popular stories on PR Daily this week

PR DAILY AWARDS
Ragan Staff

What is your health care organization's communications strategy?

JOBS OF THE WEEK
Brendan Gannon

30 jobs in the PR and marketing world

PR

Meredith L. Eaton

5 nightmares that haunt PR pros

LOAD MORE ARTICLES

Tags: Amazon, Facebook

TOPICS

SOCIAL MEDIA

MEDIA RELATIONS

CRISIS COMMUNICATIONS

MARKETING

WRITING & EDITING

WHAT WE DO

R

The New York Times

Swedish Government Scrambles to Contain Damage From Data Breach

By Christina Anderson

July 25, 2017

STOCKHOLM — Sweden's government is scrambling to contain the political fallout from a huge breach of confidential data, including the possible disclosure of the identities of undercover operatives, under the watch of a government contractor.

The breach was disclosed this month by the Swedish newspaper Dagens Nyheter, when it reported that Maria Agren, the former director general of the Swedish Transport Agency, had been fired in January for negligent handling of classified data.

The agency entered into an outsourcing agreement with IBM Sweden in April 2015, worth nearly $100 million, to manage vehicle registration and driver's license databases.

But adequate safeguards were not adopted, and as a result, unauthorized personnel at IBM subsidiaries in Eastern Europe had access to vast troves of sensitive information, including details about bridges, roads, ports, the subway system in Stockholm and other infrastructure.

In addition, the identities of people working undercover for the Swedish police and the Swedish security service, known as Sapo, may have been revealed, along with names of people working undercover for the special intelligence unit of the Swedish armed forces.

Unlike other cases involving breaches of government data, the case in Sweden does not appear to involve hacking or other malice. Instead, the focus has been on an apparent absence of proper safeguards and oversight.

On Monday, Prime Minister Stefan Lofven called the breach of information "a total breakdown." He said: "It is incredibly serious. It is a violation of the law and put Sweden and its citizens in harm's way."

Anders Thornberg, head of the Swedish Security Service, told journalists: "This is very serious because it could damage our operational business that we are conducting every day in order to protect Sweden."

Members of Parliament have not been satisfied by those assurances. On Tuesday, they interviewed Defense Minister Peter Hultqvist and Interior Minister Anders Ygeman behind closed doors, asking why Mr. Lofven was only informed of the breach in January, at least 10 months after they became aware of it.

The scandal could throw the government, which is dominated by Mr. Lofven's center-left Social Democrats, into turmoil. In a phone interview, Anna Kinberg Batra, the leader of the opposition Moderate Party, said a no-confidence vote in one or more ministers was possible.

"They have failed to communicate among themselves and to the prime minister, to the opposition and to the Swedish people," she said.

"I think the public needs to know if our national security is jeopardized or not. In my mind the minister must swiftly inform the prime minister, who apparently hadn't heard of this until this year. That is really the essence of the crisis of confidence."

According to the results of a preliminary investigation that began in January 2016, at least three unauthorized people in the Czech Republic had full access to the databases, meaning that they could copy the information and erase their electronic footprints.

The new director general of the transport agency, Jonas Bjelfvenstam, has said it will take until this fall to secure the leaked information.

Sapo urged in November 2015 that the outsourcing deal be stopped, but its recommendation was not followed, according to Dagens Nyheter.

Ms. Agren, the fired head of the transport agency, was fined $8,500 last month for being careless with sensitive information and sidestepping laws designed to protect security, privacy and details surrounding personal identity data.

Bengt Erik Angerfelt, a retired cybersecurity expert who worked with I.T. security and internet crime for the Swedish police, Sapo and Interpol, said he was not surprised by the scandal given pressures to cut costs and the ever-increasing complexity of a connected world.

“One is trying to do things as cheaply as possible and it’s expensive to hire your own personnel,” he said in a phone interview. “To do security checks on personnel in other countries is difficult.”

The head of information technology at the transport agency admitted to Sapo, the security service, that “the keys to the kingdom” had been given away, Dagens Nyheter reported on July 14, citing the preliminary investigation report by Sapo.

The transport agency manages millions of personal records and data about the infrastructure of the country’s defense. Anyone with a driver’s license, and toll-paying motorists in Stockholm, are registered, as are pilots, train conductors and air traffic controllers.

Through this information it is also possible to trace people with protected identities, armored vehicles, missing vehicles as well as where and when the transport of valuables and money are scheduled, Dagens Nyheter reported.

Ms. Agren’s sidestepping of the laws meant IBM Sweden had free rein to give access to people who had not received security clearance, it reported. It said that the project manager for the outsourcing agreement admitted during questioning that “he had no knowledge whatsoever of how to ensure security.”

IBM Sweden could not be immediately reached for comment.

S

Amazon might have a Cambridge Analytica-size problem

Amazon could be the next big tech firm to find itself in the eye of a data privacy storm.

(https://bigthink.com/reubenjackson)
REUBEN JACKSON (HTTPS://BIGTHINK.COM/REUBENJACKSON) 5 December, 2018

- This year the Cambridge Analytica scandal broke, implicating Facebook and creating mass data privacy concern.
- Concerns have been raised of Amazon user information being leaked to third parties on a regular basis.
- With the amount of sensitive information and huge number of users on the Amazon platform, this is no small concern.

2018 hasn't been a good year for Facebook. In March, the Cambridge Analytica scandal broke, implicating the company in data harvesting activities for political purposes. The story is far from over, with recent reports stating (http://www.theguardian.com/technology/2018/nov/24/mps-seize-cache-facebook-internal-papers) that the UK Parliament has seized Facebook internal company papers linked to an ongoing investigation into the matter.

Shortly after the scandal broke, Apple CEO Tim Cook twisted the knife, revealing in an interview (http://www.washingtonpost.com/news/the-switch/wp/2018/03/29/apples-tim-cook-i-would-have-avoided-facebooks-privacy-mess/?utm_term=.d9ca6213733a) with MSNBC that he believed Facebook should have shown some self-restraint. He addressed his own company's customers, stating their value to Apple and promising, "We're not going to traffic in your personal life."

Of course, the sentiment is admirable — even for hardened cynics who see the marketing angle of such a statement. However, it doesn't change the fact that all the big tech firms currently process our data inside a black box. Before the Facebook/Cambridge Analytica scandal, Google was under the microscope due to Edward Snowden's disclosures (http://www.businessinsider.com/snowden-leaks-timeline-2016-9) of NSA spying activities.

Now, Amazon could be the next big tech firm to find itself in the eye of a data privacy storm. The issue? America's biggest marketplace is heavily dependent on Chinese sellers, who are unwittingly allowing some of China's biggest payment processors access to Amazon customers' personal data.

How Chinese payment processors access Amazon user data

Amazon is a global marketplace, meaning that it's very easy for virtually anyone to become a seller on the platform. When you make an order on Amazon, your personal data including name, address, and basic credit card information and purchase details are passed through to the seller. The seller also needs to have a receiving account, so they can receive the proceeds from your purchase. Amazon requires that the receiving account is linked to the country where the seller is operating.

For this reason, many Chinese sellers use big payment processing companies based in China such as Pingpong, and Lianlian. The payment provider needs access to the seller's Amazon account to set up their receiving account, and here is where the data privacy issue occurs.

A seller has a couple of options for how a third party can plug into their Amazon account. The highest level of access is using the seller's secret key. Someone with a seller's secret key can access all the same data as the seller themselves, including customer data of people who have ordered from the seller.

Even the fact that sellers receive customer data may come as a surprise to many. After all, we assume that Amazon is the company receiving and processing our data, not some small seller on the other side of the world. However, since Amazon accepts pretty much any seller, many will need customer data to fulfill and process payment for the order.

Amazon does provide the option of using an API for payment providers to access a seller's account. However, they provide only the very thinnest of instructions to their sellers on how to do this and explain the dangers of giving out private keys in the vaguest of terms. From discussions taking place on Weixin (http://mp.weixin.qq.com/s/ZzzyTt0yO4_PbrKWo8z8yg), China's version of WhatsApp, it's apparent that Chinese sellers are being asked by payment providers to release their secret keys.

Even discussions on Amazon's own community pages imply some sellers have disclosed (https://sellercentral.amazon.com/forums/t/contradictory-advice-[illegible] their secret keys. This means that payment providers, which are huge Chinese companies, now likely have access to the customer data of a currently unquantified number of American Amazon users.

The extent of the damage

While the amount of data breached is unquantified, the sheer scale of Amazon and its ties to China provide some insights into the potential extent of the damage. There are an estimated 90 million (http://www.forbes.com/sites/louiscolumbus/2018/03/04/10-charts-that-will-change-your-perspective-of-amazon-primes-growth/#63d0af63feea) Amazon Prime subscribers in the US, with 46% of subscribers buying something at least once per week.

34% of Amazon's top sellers (http://www.marketplacepulse.com/articles/china-is-a-third-of-amazon-marketplace) are based in China, with 250,000 new Chinese sellers having joined Amazon in 2017 alone. Pingpong is just one example of a Chinese payment services provider and it has processed more than $1 billion (http://www.pymnts.com/news/ecommerce/2017/pingpong-globals-ecommerce-niche-with-smbs-chinese-economy/) worth of US payments.

Regulators have taken greater steps to intervene in matters user data privacy, but regulatory control only has a defined geographical scope. A court can hold Amazon accountable for its actions in securing customer data in its own jurisdiction, however it cannot rule against the use of data that has already leaked to foreign companies. Nevertheless, the US has been slow to introduce user privacy laws compared to the EU, which has attempted to control the issue with its far-reaching General Data Protection Regulation (GDPR.)

Because Amazon is a global company, the issue is not necessarily limited to US customer data. However, this is taking place against the backdrop of an extremely tense period in US-China trade relations. During 2018, both countries have imposed an increasing series of tariffs on imports from the other, leading to a situation which many economists believe could be extremely damaging (https://www.cnbc.com/[illegible]) to the global economy. Sectors [illegible] agriculture are being impacted by the tariffs.

It remains to be seen whether or not Amazon user data may become a pawn in the trade war between President Trump and China's leader Xi Jinping. Amazon is a US company, after all, and any misuse of US Amazon user data by Chinese companies would be likely to be seen as an attack on the US. With the famously unpredictable President Trump in charge of Chinese trade negotiations, it could go either way.

Regulators must hold big tech accountable

The privacy issues with Amazon customer data highlighted here further underline the level of trust we are placing in big tech companies. We rely on their systems, processes and overall integrity to keep our data safe. Increasingly, these firms are demonstrating that they do nothing to earn our trust.

However, once the Facebook/Cambridge Analytica scandal broke, regulators including the US Senate and the UK Parliament were quick to intervene. This has cast a shadow over Facebook's practices, and the company is finally being held to account for its actions. Perhaps it's only a matter of time before Amazon comes under the same level of scrutiny.

RELATED ARTICLES AROUND THE WEB

Amazon data breach reveals private details of customers ahead of ... › (https://www.telegraph.co.uk/technology/2018/11/21/amazon-hit-data-breach-midst-key-sales-period/)

Amazon data breach exposes customer names, emails - CBS News › (https://www.cbsnews.com/news/amazon-data-breach-exposes-customer-emails-before-black-friday/)

Amazon 'data breach' email to customers: What you should know › (https://www.clickondetroit.com/consumer/amazon-data-breach-email-to-customers-what-you-should-know)