Adobe backtracks, will refund customers after canceling their accounts

Getty Images | SOPA Images

reader comments

4 with 4 posters participating

Share this story

Adobe has reversed itself on a curious decision that would have denied refunds to customers in Venezuela whose accounts are being canceled through no fault of their own.

Adobe announced Monday that it is deactivating all user accounts in Venezuela in order to comply with an executive order issued by President Donald Trump. Adobe interpreted the executive order much more broadly than other companies, claiming that it was “unable to issue refunds” because the order required cessation of all business activity.

This was strange in part because the executive order doesn’t actually require cessation of all business activity between US companies and Venezuelan people, as it was targeted at the Venezuelan government and people who provide material support to the regime.

Additionally, Adobe was giving customers in Venezuela until October 28 to download any content they have stored in their Adobe accounts. The company didn’t explain why it could continue providing that service for a few more weeks while simultaneously being unable to issue refunds to customers who

won’t keep getting what they paid for.

Adobe reversed the no-refund part of its decision in an update to the support document yesterday. “If you purchased directly from Adobe, we will refund you by the end of the month for any paid, but unused services. We are working with our partners on the same,” Adobe said in the update.

Adobe also reversed itself on one other portion of the mass account deletion. Adobe originally said it would have to stop providing both fee-based and free services to people in Venezuela. But now, Adobe says its free Behance social media platform will continue to be available in Venezuela after the cutoff date for other services.

“In order to remain compliant, Adobe will be deactivating all accounts in Venezuela, with the exception of Behance, on October 29, 2019,” Adobe said.

Trump’s executive order, titled “Blocking Property of the Government of Venezuela,” was a response to Venezuela’s ongoing presidential crisis following a disputed election held in May 2018. The US supports Juan Guaidó’s claim to the presidency and describes President Nicolás Maduro as a usurper, saying the US is trying to “isolate Maduro’s illegitimate regime from the global financial system and the international community.”

https://arstechnica.com/?p=1582803

FBI misused surveillance

data, spied on its own, FISA ruling finds

Enlarge / FBI agents ran queries across thousands of US individuals, including potential sources and anyone with access to FBI facilities, against raw metadata from FISA-authorized bulk collection databases.
Bloomberg via Getty Images

reader comments

46 with 42 posters participating

Share this story

In an October 2018 ruling unsealed and posted on October 8, 2019 by the Office of the Director of Intelligence, the United States Foreign Intelligence Surveillance Court (FISC) found that the employees of the Federal Bureau of Investigation had inappropriately used data collected under Section 702 of the Foreign Intelligence Surveillance Act (FISA). The FBI was found to have misused surveillance data to look into American residents, including other FBI employees and their family members, making large-scale queries that did not distinguish between US persons and foreign intelligence targets.

The revelation drew immediate outcry from privacy advocates and renewed calls for the termination of FISA and USA FREEDOM Act that authorized bulk intelligence collection. President Donald Trump signed a bill extending Section 702 collection authorizations for six years in 2018; the Office of the Director of National Intelligence announced earlier this year that the administration would seek the extension of authority for collection of call data granted under the USA FREEDOM Act.

In a statement emailed to Ars Technica, ACLU Senior Legislative Counsel Neema Singh Guliani, said:

> *The government should not be able to spy on our calls and emails without a warrant. Any surveillance legislation considered by Congress this year must include reforms that address the disturbing abuses detailed in these opinions. Congress and the courts now have even more reason to prohibit warrantless searches of our information, and to permanently close the door on any collection of information that is not to or from a surveillance target.*

Let me Intel-Google that

The Foreign Intelligence Surveillance Court ruling found that the FBI's "querying procedures" for intelligence data did not properly record when the database of intelligence data was searched for information about US persons. "The querying procedures did not require FBI personnel to document the basis for finding that each United States-person query term satisfied the relevant standard—i.e., that queries be reasonably designed to return foreign-inteligence information or evidence of crime," the FISC opinion stated. "Without such documentation and in view of reported instances of non-compliance with that standard, the procedures seemed unreasonable under FISA's definition of 'minimization procedures' and possibly the Fourth Amendment."

Among those instances of "non-compliance" were:

- Between March 24 and 27, 2017, the FBI ran queries against intelligence data "using identifiers for over 70,000 communications facilities 'associated with' persons with access to FBI facilities and systems," the court noted, "notwithstanding advice from the FBI Office of General Counsel (OGC) that they should not be conducted without the approval of the OGC and the

National Security Division of the Department of Justice."

- On December 1, 2017, a redacted FBI division "conducted over 6,800 queries using the Social Security Numbers of individuals" against raw, unredacted FISA data. A week later, the same unit conducted 1,600 queries using another set of identifiers for US persons. The person who conducted the queries "advised he did not intend to run them against raw FISA information, but nonetheless reviewed raw FISA information returned by them."
- In February of 2018, the FBI searched raw FISA data for information, with about 30 queries regarding "potential [redacted] sources," and conducted about 45 other queries on people "under consideration as potential sources of information."
- In an undated event, reported to the Department of Justice's National Security Division in April of 2018, the FBI ran queries against raw FISA metadata using identifiers for "approximately 57,000 individuals" where it was not clear that the information would return foreign intelligence information.
- Queries against individual US persons were run against the FISA data on a number of occasions, including people about to be served a FISA order—and "a small number of cases in which FBI personnel apparently conducted queries for improper personal reasons—for example, a contract linguist who ran queries on himself, other FBI employees, and relatives."

The court found a huge lack of oversight over the FBI's querying of FISA metadata and ordered the FBI to revise its search procedures. The FISC ruling said that the FISA statutory and Fourth Amendment concerns regarding warrantless searches would be cleared if all queries required written documentation of the basis for a belief by the FBI that searching against a US person's metadata would be "reasonably likely to return foreign-intelligence information or evidence

of crime” before anyone at the FBI was allowed access to the contents of FISA data that would be returned by such a search.

https://arstechnica.com/?p=1582117

Twitter transgression proves why its flawed 2FA system is such a privacy trap

reader comments

106 with 84 posters participating

Share this story

If ever there was a surefire way to sour users against a two-factor authentication system that was already highly flawed, Twitter has found it. On Tuesday, the social media site said that it used phone numbers and email addresses provided for 2FA protection to tailor ads to users.

Twitter requires users to provide a valid phone number to be eligible for 2FA protection. A working cell phone number is mandatory even when users’ 2FA protection is based solely on security keys or authenticator apps, which don’t rely on phone numbers to work. Deleting a phone number from a user’s Twitter settings immediately withdraws an account from Twitter 2FA, as I confirmed just prior to publishing this post.

Security and privacy advocates have long grumbled about this requirement, which isn’t a condition of using 2FA protection from Google, Github, and other top-ranked sites. On Tuesday, Twitter gave critics a new reason to complain. The site said it may have inadvertently used email addresses and phone numbers provided for 2FA and other security purposes to match users to marketing lists provided by advertisers. Twitter didn’t say if the number of users affected by the blunder was in the hundreds or the millions or how long the improper targeting lasted.

Company officials wrote:

> *We cannot say with certainty how many people were impacted by this, but in an effort to be transparent, we wanted to make everyone aware. No personal data was ever shared externally with our partners or any other third parties. As of September 17, we have addressed the issue that allowed this to occur and are no longer using phone numbers or email addresses collected for safety or security purposes for advertising.*

Security advocates, including Matt Green—a Johns Hopkins professor specializing in cryptography—wasted no time castigating Twitter for the gaffe.

“In all seriousness: whose idea was it to use a valuable advertising identifier as an input to a security system,” he wrote on Twitter. “This is like using raw meat to secure your tent against bears.”

> *In all seriousness: whose idea was it to use a valuable advertising identifier as an input to a security system. This is like using raw meat to secure your tent against bears.*
>
> *— Matthew Green (@matthew_d_green) October 8, 2019*

Not all 2FA was created equal

Two-factor authentication has emerged as the single-most effective means for protecting accounts against phishing and so-called credential-stuffing attacks (the latter uses passwords swept up in breaches on one site to guess passwords on unrelated sites). As the name suggests, 2FA requires a factor—for example, a security key or a fingerprint—in addition to a password to successfully log in from a device that has never accessed the account before.

Over the past few years, security practitioners have increasingly turned away from 2FA based on SMS text messages. The reasons: (1) attackers can take control of users’ phone numbers by impersonating the owners and getting the carrier to swap out the SIM card, and (2) SMS messages can be hijacked through weaknesses in the Signalling System No. 7 routing protocol that cellular carriers use to make their networks interoperable. Attackers have been known to actively exploit these weaknesses more than once. A far more effective means of 2FA relies on physical security keys that connect over USB or NFC interfaces or—less secure but still better than SMS—one-time passwords generated by authenticator apps. Twitter allows either form of 2FA. Both require a user to provide a phone number.

Twitter signals a change is coming

Twitter representatives declined to answer on the record why a phone number is required to use 2FA. A representative on background, however, said that the requirement is based on previous experiences in which users frequently lost access to other 2FA methods and were locked out of accounts with no way to recover. Twitter officials now recognize that tying 2FA to a phone number isn't ideal, and they are looking for ways to decouple the two in the future.

Last year, Facebook was outed for using 2FA-provided phone numbers to send notifications that weren't related to security. The social network said the behavior was the result of a bug.

While SMS-based 2FA isn't ideal, it's still better for most people than no 2FA at all—at least when services don't use phone numbers for marketing purposes.

https://arstechnica.com/?p=1582055

Senator proposes mandatory labeling for products with mics, cameras

Enlarge / A surveillance camera on display in Hamburg, Germany, in January 2019.

reader comments

131 with 69 posters participating

Share this story

Much in the same way that food labels are now required to disclose the potential presence of allergens such as peanuts, one Senator is proposing a law that would require tech companies to include a label on products disclosing the presence of recording devices.

The bill, dubbed the Protecting Privacy in our Homes Act, would mandate a new kind of labeling on goods that include Internet-connected microphones or cameras. The proposed law does not define what kind of labels would need to be appended but rather would order the Federal Trade Commission to put in place specific regulations "under which each covered manufacturer shall be required to include on the packaging of each covered device manufactured by the covered manufacturer a notice that a camera or microphone is a component of the covered device."

Sen. Cory Gardner (R-Colo.) introduced the bill to the Senate. "Consumers face a number of challenges when it comes to their privacy, but they shouldn't have a challenge figuring out if a device they buy has a camera or microphone embedded into it," Gardner said. "This legislation is about consumer information, consumer empowerment, and making sure we're doing everything we can to protect consumer privacy."

Most products that ship with cameras or microphones included tout the inclusion of such recording devices as a selling point, which could make this kind of regulation feel redundant at best. That said, there's quite a difference between "most" and "all." A rule such as the regulation Gardner proposes would close the gap that, for example, led owners of Nest Secure devices to the unpleasant discovery earlier this year

that the products had shipped with undisclosed microphones.

Gardner is a co-chair of the Senate Cybersecurity Caucus, along with Sen. Mark Warner (D-Va.). The two earlier this year led a bipartisan group of senators that co-sponsored the Internet of Things Cybersecurity Act of 2019, which would require existing regulators to develop security standards for connected devices.

The Senate, however, largely seems concerned with other events this year, and GovTrack.us gives the PPHA a 3% chance of actually becoming law.

https://arstechnica.com/?p=1581691

Blizzard bans pro Hearthstone gamer for statement supporting Hong Kong

Enlarge / Ng “Blitzchung” Wai Chung declares his support for Hong Kong while two announcers duck behind their desks.

reader comments

312 with 200 posters participating

Share this story

Blizzard has stripped a Hong Kong professional *Hearthstone* player of his tournament prize money and banned him from

tournament play for a year after he expressed support for Hong Kong during the livestream of a *Hearthstone* game. Blizzard said that the actions of Ng "Blitzchung" Wai Chung violated Section 6.1 of the tournament's rules, which prohibits players from doing anything that "offends a portion or group of the public."

"Grandmasters is the highest tier of *Hearthstone* Esports and we take tournament rule violations very seriously," Blizzard wrote. "While we stand by one's right to express individual thoughts and opinions, players and other participants that elect to participate in our esports competitions must abide by the official competition rules."

Blizzard has deleted the video from its video-on-demand service. But gaming news site Inven Global posted the offending portion to Twitter. According to Inven Global, Blitzchung shouted, in Chinese, "Liberate Hong Kong, revolution of our age!" He also donned a gas mask, a symbol of the Hong Kong protestors.

Blitzchung appeared to be egged on by the two announcers on the livestream, who laughed and ducked behind their desk as he made his statement. Blizzard says it has fired the two announcers.

"There are serious protests in my country now," Blitzchung said in a statement to Inven Global. "My call on stream was just another form of participation of the protest that I wish to grab more attention."

"I put so much effort in that social movement in the past few months that I sometimes couldn't focus on preparing my Grandmaster match," he added. "I know what my action on stream means. It could cause me lot of trouble, even my personal safety in real life. But I think it's my duty to say something about the issue."

China uses its economic heft to censor Hong Kong supporters

The status of Hong Kong is a sore subject for the Chinese government. Hong Kong has been part of China since the 1997 handover from British control. But the Chinese government promised to maintain a policy of “one country, two systems,” respecting the greater freedoms enjoyed in Hong Kong until at least 2047.

But many Hong Kongers believe the mainland government hasn’t kept its promise. As a result, the territory has been convulsed by protests in recent months. Protests initially focused on legislation that would allow extraditions from Hong Kong to the mainland, but protestors’ demands have broadened over time. The protestors are now demanding democratic election of Hong Kong’s leaders. Currently, the island’s convoluted electoral process gives the mainland the de facto ability to choose Hong Kong’s leaders.

In recent days, China has been using its economic power to pressure Western companies into censoring pro-Hong Kong speech. Last Friday, Daryl Morey, general manager of the Houston Rockets (popular in China since it drafted Chinese star Yao Ming), tweeted the slogan “Fight for Freedom, Stand with Hong Kong.”

The Chinese government reacted with fury. China’s state broadcaster said it would suspend broadcasts of NBA preseason games played in China. The Rockets lost Chinese sponsorship deals. Morey quickly deleted his tweet. The NBA responded with a groveling statement recognizing that Morey’s comments “deeply offended” people in China, stating that Morey’s words don’t reflect the views of the NBA or the Rockets and adding that the NBA had “great respect for the history and culture of China.” (NBA commissioner Adam Silver later struck a more defiant tone, stating “we are not apologizing for Daryl

exercising his freedom of expression.”)

The lesson here is that any Western company making significant investments in China is potentially exposing itself to this kind of relationship. Some Western companies have stayed out of China due in part to human rights concerns. Google, for example, pulled out of the Chinese market in 2010. Earlier this year, the company officially canceled plans to launch a censored Chinese version of its search engine after protests inside and outside the company.

https://arstechnica.com/?p=1581779

Adobe cancels all user accounts in Venezuela to comply with Trump order

Enlarge / Adobe Creative Cloud application icons.
Getty Images | Bloomberg

reader comments

224 with 135 posters participating

Share this story

Adobe is deactivating all user accounts in Venezuela, saying that the action is necessary to comply with an executive order issued by President Donald Trump. The action affects both free and paid accounts.

In an FAQ titled “Adobe compliance with US Executive Order,” the company explained yesterday why it is canceling its Venezuela-based customers’ subscriptions:

> *The US Government issued Executive Order 13884, the practical effect of which is to prohibit almost all transactions and services between US companies, entities, and individuals in Venezuela. To remain compliant with this order, Adobe is deactivating all accounts in Venezuela.*

Adobe appears to be interpreting the executive order more broadly than other companies. Microsoft’s Office 365 and other cloud services are still available in Venezuela, for example. The executive order itself says the US action is targeted at the Venezuelan government and people who provide material support to the regime.

A US government notice states that the order does not affect all commerce between the US and Venezuela. “US persons are not prohibited from engaging in transactions involving the country or people of Venezuela, provided blocked persons or any conduct prohibited by any other Executive order imposing sanctions measures related to the situation in Venezuela, are not involved,” the notice says. (In this context, a “person” is an individual or an entity such as a corporation or other type of organization.)

Adobe won’t give refunds

Adobe says it has no idea when or if it will reactivate customer accounts. “Executive Order 13884 was issued with no expiration date—the decision to rescind it rests solely with the US Government,” Adobe wrote. “We will continue to monitor developments closely and will make every effort to restore services to Venezuela as soon as it is legally permissible to do so.”

According to Adobe, the company is not allowed to provide refunds. “We are unable to issue refunds. Executive order 13884, orders the cessation of all activity with the entities including no sales, service, support, refunds, credits, etc.,” Adobe said.

Adobe is giving users in Venezuela until October 28 to download any content they have stored in their Adobe accounts. Files can be downloaded from Creative Cloud, Lightroom, Document Cloud, and Adobe Spark.

As previously mentioned, Adobe’s action will cut off access to users with either paid subscriptions or free accounts. “Adobe will no longer provide access to software and services, including free ones, or enable you to make any new purchases,” the company said.

Adobe said it might take the same action in other countries. To comply, Adobe said it is “ceasing all activity with entities and individuals in Venezuela as well as those who otherwise meet the criteria of Executive Order 13884 or other US sanctions regulations.”

The Trump order

Trump’s executive order, issued on August 5, was titled, “Blocking Property of the Government of Venezuela.” The order was a response to Venezuela’s ongoing presidential crisis following a disputed election held in May 2018.

The US supports Juan Guaidó’s claim to the presidency and describes President Nicolás Maduro as a usurper. The White House said Trump’s executive order is intended to “isolate Maduro’s illegitimate regime from the global financial system and the international community.”

As the Washington Post wrote in August, the Trump order “blocks all property and assets of the government and its

officials, and prohibits any transactions with them, including the Venezuelan Central Bank and the state oil company."

There was disagreement among experts on how wide-ranging the executive order is. "This is not an embargo. It does not create penalties for business with Venezuela altogether, it just denies such activities with the government of Venezuela, and it is doubtful there were any of those still extant to be cut off by this action," former State Department official Richard Nephew told The New York Times in August.

"In theory, a US company can continue to deal with non-governmental companies in Venezuela, and we do not believe the US will be inclined to sanction privately owned Venezuelan companies," the National Law Review wrote.

However, Venezuelan economist Francisco Rodríguez told the Times that "financial institutions will be cautious not to make dealings with Venezuelan private sector firms, which could be perceived as proxies for the Venezuelan government."

https://arstechnica.com/?p=1581805

Inexpensive, unpatched phones put billions of users' privacy at risk

Enlarge / Cellphones charging in the Philippines at a station run by generator in 2013, while power was out in the wake of tyhpoon Haiyan.

reader comments

116 with 65 posters participating, including story author

Share this story

Privacy, it seems, is increasingly a luxury reserved for those who can afford it. “Free” services are rarely free, and in the 21st century, the adage seems to be that if you aren’t paying with your money, you’re paying with your personal data. But while a user at the higher ends of the income scale can afford to be choosy with both their cash and their privacy, users of the cheap, mostly Android-based smartphones that dominate the market worldwide are bearing the burden.

Apple’s iPhone might be the single most popular device line among US consumers, but the iPhone’s high-end cachet comes with a matching price tag. Likewise, a premium flagship Android phone, such as a new Google Pixel or Samsung Galaxy device, runs in the $500 to $1000 range.

Connectivity, however, is happily not limited to just the global wealthy. Billions of users in both developing and mature economies to whom the price tag puts a high-end phone out of reach still have access to lower-spec devices. Nearly all of the lower-end phones available worldwide run Android, giving Google’s OS a greater than 80% market share globally.

Android is easily modifiable by device manufacturers and wireless carriers, and the cheaper the phone is, the more likely it is that someone, or multiple someones, has installed crapware or malware on it, Fast Company reports.

Fast Company highlights one example: the MYA2 MyPhone, sold in the Philippines. The phone as described is a privacy and security nightmare:

> *First, it comes with an outdated version of Android with known security vulnerabilities that can’t be updated or*

> *patched. The MYA2 also has apps that can't be updated or deleted, and those apps contain multiple security and privacy flaws. One of those pre-installed apps that can't be removed, Facebook Lite, gets default permission to track everywhere you go, upload all your contacts, and read your phone's calendar.*

The wealth gap

According to data gathered by the Pew Research Center, about 17% of US adults use smartphones and *only* smartphones to connect to the Internet. The farther down the household-income ladder you go, the higher that percentage is. Among those whose household income falls between $50,000 and $75,000, about 10% of users are mobile-only. Among those whose household incomes fall below $30,000, the figure rises to 26%.

Fast Company points to a recently published study conducted by researchers at the University of Pennsylvania and Rutgers University. The study finds that many mobile-only, lower-income consumers were well aware that their privacy was regularly being violated, but they didn't feel they had a real choice.

"Nearly all study participants shared stories of relinquishing their data privacy, which the researchers consider to be a basic human right, in exchange for the ability to access online services and platforms," the researchers wrote. "Many people shared anecdotes about forgoing opportunities in an attempt to maintain data privacy."

The researchers concluded:

> *Because of the sheer ubiquity of digitized data compiled on individuals who rely on cell phones to access the Internet, the need for privacy should be elevated from a personal liberty and legal right to a matter of social justice… Data*

> *privacy is not a luxury for those who cannot afford to invest the time, resources, and effort required to actively protect one's digital assets.*

Global challenge

Fast Company notes that approximately 2 billion users, or just over half of all people now online, only access the Internet on their smartphones. That number is projected to be as high as 3.7 billion users by 2025, as mobile infrastructure solidifies a foothold and gains penetration in currently underserved regions.

The problem is not new, and it's not limited to users in developing economies or low-GDP nations. In 2016, for example, 120,000 Android phones distributed inside the US by BLU Products were found to be sending users' text messages and other highly sensitive data to China. The security hole was not a bug but a feature of the phones—the phones just weren't meant to be distributed that way inside the United States.

(BLU reached a settlement with the Federal Trade Commission in April 2018.)

Dozens of other models of Android phones have been found in recent years to arrive pre-loaded with malware or boasting backdoors that should not be—particularly phones distributed by low-cost resellers.

And the trade-off isn't always surreptitious. In 2016, for example, Amazon launched a program selling cheap, unlocked Android phones with "special offers" (i.e. advertisements) baked into the lock screen and certain pre-installed apps. The company dumped the program in 2018 after Google changed the terms of its developer policy.

https://arstechnica.com/?p=1581257

Hospitals that are turning away patients reportedly pay ransomware attackers

reader comments

63 with 47 posters participating

Share this story

Three Alabama hospitals have paid a ransomware demand to the criminals who waged a crippling malware attack that’s forcing the hospitals to turn away all but the most critical patients, the Tuscaloosa News reported.

As reported last Tuesday, ransomware shut down the hospitals’ computer systems and prevented staff from following many normal procedures. Officials have been diverting non-critical patients to nearby hospitals and have warned that emergency patients may also be relocated once they are stabilized. An updated posted on Saturday said the diversion procedure remained in place. All three hospitals are part of the DCH health system in Alabama.

Over the weekend, the Tuscaloosa News said DCH officials made a payment to the people responsible for the ransomware attack. The report didn’t say how much officials paid. Saturday’s statement from DCH officials said they have obtained a decryption key but didn’t say how they obtained it.

The statement read in part:

> *In collaboration with law enforcement and independent IT security experts, we have begun a methodical process of system restoration. We have been using our own DCH backup files to rebuild certain system components, and we have obtained a decryption key from the attacker to restore access to locked systems.*
>
> *We have successfully completed a test decryption of multiple servers, and we are now executing a sequential plan to decrypt, test, and bring systems online one-by-one. This will be a deliberate progression that will prioritize primary operating systems and essential functions for emergency care. DCH has thousands of computer devices in its network, so this process will take time.*
>
> *We cannot provide a specific timetable at this time, but our teams continue to work around the clock to restore normal hospital operations, as we incrementally bring system components back online across our medical centers. This will require a time-intensive process to complete, as we will continue testing and confirming secure operations as we go.*

DCH representatives didn’t respond to an email seeking details and comment for this post.

To pay or not to pay

Law enforcement officials and security professionals generally discourage ransomware payments because such payments encourage more attacks, and there is no guarantee the criminals will produce the key as promised. And even when criminals do produce a key, sometimes the malware can permanently destroy some of the encrypted data. According to a FAQ published by DCH, the strain of ransomware that hit the hospitals is known as Ryuk, which specializes in burrowing deep into infected

networks to exact big payments.

“Ryuk is particularly nasty as the code contains bugs that causes it to damage about one in every eight files that it encrypts,” Brett Callow, a spokesman with security firm Emsisoft, told Ars. “So there is almost always data loss in these cases even when the ransom is paid.”

Emsisoft provides free tools it says can often decrypt data that’s hit by ransomware. But even when it’s successful against Ryuk, those tools don’t enable corrupted files to be recovered.

The darker side of not paying ransoms is this: often, organizations hit by ransomware end up paying much higher costs when they choose to rebuff the demands. Instead, they attempt to rebuild crippled networks on their own. The city of Baltimore, for example recently paid more than $18 million to restore its ransomware-crippled network. The criminals in that attack had demanded $70,000, but both city and FBI officials discouraged the payment.

The rise of ransomware over the past five years underscores the importance of having a robust and reliable backup system that IT personnel can use in the event a ransomware attack or some other serious event wipes out data. As it turns out, backup regimens are often not as robust as they should be, and even when they are, restoring networks solely from backups can still be costly and time-consuming.

https://arstechnica.com/?p=1581299

The broken record: Why Barr’s call against end-to-end encryption is nuts

Enlarge / The US, UK, and Australia want Facebook to hold off on end-to-end encrypting Messenger until they have a way to inject themselves into the conversation.
picture alliance / Getty Images

reader comments

141 with 108 posters participating

Share this story

Here we go again.

US Attorney General William Barr is leading a charge to press Facebook and other Internet services to terminate end-to-end encryption efforts—this time in the name of fighting child pornography. Barr, acting Secretary of Homeland Security Kevin McAleenan, Australian Home Affairs Minister Peter Dutton, and United Kingdom Secretary of State Priti Patel yesterday asked Facebook CEO Mark Zuckerberg to hold off on plans to implement end-to-end encryption across all Facebook Messenger services “without including a means for lawful access to the content of communications to protect our citizens.”

The open letter comes months after Barr said in a speech that “warrant-proof” cryptography is “extinguishing the ability of law enforcement to obtain evidence essential to detecting and investigating crimes” and allowing “criminals to operate with impunity, hiding their activities under an impenetrable cloak of secrecy.” The new message echoes a joint communiqué issued

by the US, UK, Australia, Canada and New Zealand (the "Five Eyes") from July, which stated:

> *…it is imperative that all sectors of the digital industry including Internet Service Providers, device manufacturers and others to continue to consider the impacts to the safety of children, including those who are at risk of exploitation, when developing their systems and services. In particular, encryption must not be allowed to conceal or facilitate the exploitation of children.*

Facebook has played a significant policing role on social media, providing reports of child abuse imagery and attempts by offenders to groom children online to the National Center for Missing and Exploited Children (NCMEC) in 2018, for instance. And there is no doubt the child pornography problem has exploded in recent years. A recent New York Times report revealed that the number of images of sexual abuse of children has been growing exponentially over the past two decades, with investigators flagging over 45 million images and videos last year. Facebook's reports were 90 percent of the 18.4 million cases reported to NCMEC in 2018—a number double that of 2017 and 18 times greater than the number reported in 2014.

Barr and his cohorts noted that NCMCE "estimates that 70% of Facebook's reporting—12 million reports globally" for content related to child sexual exploitation and terrorism "would be lost" if all Messenger traffic is protected by end-to-end encryption and Facebook cannot screen the content through its safety systems. "This would significantly increase the risk of child sexual exploitation or other serious harms," Barr and the others claimed.

The letter also broadened its message beyond Facebook to the entire tech industry, stating:

> *We therefore call on Facebook and other companies to take the*

following steps:

- *Embed the safety of the public in system designs, thereby enabling you to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims;*
- *Enable law enforcement to obtain lawful access to content in a readable and usable format;*
- *Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences your design decisions; and*
- *Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational.*

There are some major problems with this plan. First, backdoored encryption is fragile at best and likely to be quickly broken. Second, encryption is available in enough forms already that blocking its use by major service providers won't stop criminals from encrypting their messages. If secure encryption is a crime, only criminals will have secure encryption—and it will be really easy to be a criminal, since all it takes is a download or some simple mathematics.

The stupid criminal argument

Much of the reasoning behind the need to prevent end-to-end encryption by default—an argument used when Apple introduced it as part of iMessenger and repeated multiple times since—is that criminals are inherently stupid, and giving them protection by default protects them from being stupid and not using encryption.

Facebook has offered end-to-end encryption as an option for Messenger conversations for years now, and it offers the service as part of WhatsApp as well. But because encryption

requires an extra (and non-intuitive) step to turn it on for Messenger, most people don't use it—apparently even criminals sending messages they think aren't under surveillance. It's like the Dunning-Kreuger effect in that case—the belief is that criminals think they're "using the juice" and it's concealing them from being observed.

The problem is not all criminals are idiots. And while Facebook may have contributed massively to the reporting of child pornography in recent years, there are other services that even the idiots could move to if it becomes apparent that they're not out of sight. Take Telegram, for instance—where much of 8chan moved to after the site lost its hosting—or WhatsApp or Signal, which provide end-to-end voice and messaging encryption. On top of those, there are a host of "dark Web" and "deep Web" places where criminals, including those exploiting children, operate.

Based on conversations I've had with researchers and people in law enforcement, there is a significant amount of tradecraft related to these types of crimes floating around in forums. Not all of it is very good, and people get caught—not because they didn't have end-to-end encryption but because they used it with the wrong person.

Laws don't change mathematics

Four years ago, when the focus was on catching terrorists instead of child pornographers, then-FBI Director James Comey decried the "cynicism" toward government spying and insisted that mathematicians and computer scientists just hadn't tried hard enough to create encryption with a "golden key" for law enforcement and intelligence organizations. But as I pointed out then, all you have to do is look at what happened when the US government tried to push backdoored encryption onto phone communications in the 1990s to understand why a government-mandated backdoor would be risky at best. As Whitfield Diffie

(half of the pair who brought us the Diffie-Hellman Protocol for encryption key exchange) put it in 1993 when warning against implementing key escrow and the "Clipper Chip":

- *The backdoor would put providers in an awkward position with other governments and international customers, weakening its value*
- *Those who want to hide their conversations from the government for nefarious reasons can get around the backdoor easily*
- *The only people who would be easy to surveil would be people who didn't care about government surveillance in the first place*
- *There was no guarantee someone else might not exploit the backdoor for their own purposes*

To reinforce these points, a group of leading computer science and cryptography researchers—including some who actually broke the Clipper Chip's key escrow scheme in 1997—published a paper in 2015 warning yet again against government backdoors in encryption. These researchers noted they could create vulnerabilities in systems exploitable by people other than warrant-bearing, lawful searchers:

> *The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard-to-detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult questions about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.*

The math and science of encryption has not stopped government from trying to change the rules, however. While Barr lacks the

legal backing to force Facebook or other companies to comply with his demand, other members of the Five Eyes are pressing their fight against encryption with legal teeth.

Last December, Australia passed a law that mandates government backdoors into encrypted communications, dictating that service and application providers must be able to provide access on demand to individuals' messages. While a similar effort four years ago in the United Kingdom failed, the UK has mandated Web blocking technologies to fight child pornography and other content-oriented crimes—and the country could conceivably extend that blocking to companies that provide encrypted communications seen as a means for trafficking child exploitation.

Other tools in the bag

In many ways, the arguments about end-to-end encryption seem moot—considering that law enforcement and intelligence organizations already have so many other ways to watch for illicit activities and target suspects. DNS traffic, targeted warrants, and other legal vehicles to gain access to accounts (as with the still-active PRISM program), the targeting of hidden services on Tor (as with the CyberBunker 2.0 bust last month), and end-point hacking all give officials a lot to work with without having to break the rest of the Internet in the process.

While fighting child exploitation, terrorism, or any other fundamental evil is vitally important, the risks posed by banning encrypted communications between citizens, customers and businesses, journalists and sources, whistleblowers and lawyers, and every other legal pairing of entities who may have some need to communicate in confidence are too high to justify mandating an untenable, universal, extraordinary level of access for government to communications.

Every US presidential administration for the past 50 years has

demonstrated in some way why we should be concerned about abuse of surveillance powers. And we know from Edward Snowden just how expansive those powers have grown. That’s part of the reason that Internet services have moved so decisively toward providing end-to-end encryption and removing themselves from the surveillance apparatus.

https://arstechnica.com/?p=1580075

Microsoft says Iranian hackers tried to hack a US presidential campaign

reader comments

82 with 45 posters participating

Share this story

Hackers backed by the Iranian government recently tried to hack email accounts used by the campaign of a US presidential candidate, a Microsoft official said on Friday.

The “Phosphorous” hackers, as Microsoft has named the group, targeted the unidentified campaign by attempting to access email accounts campaign staff received through Microsoft cloud services. Rather than relying on malware or exploiting software vulnerabilities, the attackers worked relentlessly to gather information that could be used to activate password

resets and other account recovery services Microsoft provides.

“Highly motivated”

The attacks on the campaign were part of a major offensive by Phosphorous that—over a 30-day period from August to September—made more than 2,700 attempts to identify consumer email accounts belonging to targeted individuals. Besides campaign staff, targeted accounts also belonged to current and former US government officials, journalists covering global politics, and prominent Iranians living outside of Iran. Of the more than 2,700 attempts to identify accounts, 241 of them were attacked. The attacks resulted in the successful compromise of four accounts, none of which belonged to the campaign.

“While the attacks we’re disclosing today were not technically sophisticated, they attempted to use a significant amount of personal information both to identify the accounts belonging to their intended targets and in a few cases to attempt attacks,” Tom Burt, Microsoft’s corporate vice president of customer security and trust, wrote in a post. “This effort suggests Phosphorous is highly motivated and willing to invest significant time and resources engaging in research and other means of information gathering.”

According to Burt, here’s how the account takeover attempts worked:

> *Phosphorous used information gathered from researching their targets or other means to game password reset or account recovery features and attempt to take over some targeted accounts. For example, they would seek access to a secondary email account linked to a user’s Microsoft account, then attempt to gain access to a user’s Microsoft account through verification sent to the secondary account. In some instances, they gathered phone numbers belonging to their targets and used them to assist in authenticating password*

resets.

In July, Microsoft said that in the previous 12 months, it notified almost 10,000 customers that they had been targeted or compromised by nation-sponsored hackers. Chief among the hacking groups were Holmium and Mercury, both of them codenames for distinct groups backed by Iran's government. Other attacks were sponsored by the governments of Russia and North Korea. About 84 percent of the attacks targeted large "enterprise" organizations such as corporations, with the remaining 16 percent hitting consumers.

Gird your loins

Burt on Friday called on Microsoft customers to enable two-step verification (2SV) to protect their accounts. The most robust form of 2SV requires users to have a physical security key such as a Yubikey from Yubico. Before an account can be accessed from a new computer or phone, the user must plug the key into a USB slot, or connect to the device over NFC or Bluetooth Low Energy. A useful, though less effective form of 2SV requires short-lived one-time passwords that are fed from an authenticator app installed on a user's phone.

Burt also reminded users to periodically check the login history of their accounts. If there are logins from unrecognized devices of IP addresses, you can notify Microsoft by clicking a "Secure Your Account" link. Both the 2SV and login history features can be accessed in the Account Security settings.

Accounts that are part of a political campaign, political party committee, or non-governmental organization or think tank related to democracy are eligible for AccountGuard. The feature provides monitoring and a unified threat notification service across all the Office 365 accounts for both work and personal use. More than 60,000 accounts in 26 countries are

currently enrolled. To date, Microsoft has issued more than 800 notifications of attempted nation-state attacks to AccountGuard members, up from 781 in July.

https://arstechnica.com/?p=1580103