Fall 12-15-2017

Personal Privacy And Data Security In The Age Of The Internet

Alexandra Langone
Cuny Graduate School of Journalism

We Talked to Security Experts About How to Protect Your Online Data. Here's What They Said

By Alix Langone

If you're one of the millions of Americans feeling like it's time to start better protecting your personal data, you're pretty much out of luck, according to cybersecurity experts.

The recent data-sharing controversy surrounding [f500link ignore=true]Facebook[/f500link] and its failure to prevent improper data harvesting by Cambridge Analytica is only the tip of the iceberg when it comes to the ways both corporate data sharing and corporate hacks affect ordinary people's lives.

The ongoing [f500link]Facebook[/f500link] scandal is just one of many incidents related to data overreaches and breaches that have recently jeopardized millions of Americans' personal information. The information lost includes everything from names and contact information to more sensitive data, like social security numbers. There have been dozens of major corporate hacks in the past few years, ranging from headline-grabbing hacks like the Uber data breach that exposed 57 million customers' information, to breaches at LinkedIn, [f500link]Target[/f500link], JPMorgan and more. At this point, virtually no industry remains untouched by hackers, who usually steal consumer data for financial gain by selling it on the dark web.

But while all the attacks ultimately have the same end result — people's personal information is put at risk — there is a big difference between companies being hacked by third parties (Uber, Target, Equifax) and companies voluntarily sharing information with or selling information to third parties (Facebook).

"Comparing Facebook to Equifax, Facebook takes significant effort to avoid being breached. They spend a significant amount of time and money focusing on not being breached," said Michael Borohovski, co-founder of Tinfoil Security, a company that monitors website security. "Facebook was not a failure of security, it was a failure of maturity or ethics — whereas Equifax was negligent in terms of a failure of information security."

When asked what people can do to prevent their data from being harvested without their direct knowledge, security technologist Bruce Schneier's answer was chillingly straightforward.

"You can't do anything. That's the fundamental problem with this," he said.

And he's not the only one. MONEY talked to a handful of cybersecurity experts and all of them agreed people have little to no power over their personal information once it's in the hands of a third party. (To be clear, it's still a good idea to follow cybersecurity best practices like using complex passwords, never repeating the same password for different services, and using two-factor authentication whenever possible.)

Why is it so hard to protect your personal data from being collected without your knowledge?

Schneider pointed the finger at Uncle Sam, saying the U.S. has no laws in place to regulate data brokerage companies and what is known as "surveillance capitalism," a new kind of business model in which corporations profit off of people's personal data. And he says the only way consumers can take control of their personal information to prevent it from being used by companies to make profits is by demanding change at the legal and regulatory level.

“You live in the United States and the United States doesn’t regulate surveillance capitalism. Your data can be bought and sold without your knowledge and consent. That’s the way it works," he said. "If you don’t like that, lobby your congressman. That is your only option.”

Schneier argues that these non-consensual data grabs aren’t a bug inside corporate data collections — they are a feature. "Their business model is collecting your data without your knowledge and consent and selling it to companies who want to manipulate you with it,” he said. "That’s their business model. And it’s a legal business model.”

What he means is that when you sign up for services like Uber or Facebook, you're usually prompted to accept that company's terms and conditions by checking off an "I have read and agree" box, otherwise you can't use the service. This concept is called mandated disclosure, and it's inherently problematic for consumers because you're required to sign away your rights to your own information in order to engage with a product.

And signing it makes whatever that company decides to do with your data completely legal. Companies get away with using mandated disclosures for two reasons: There are no federal laws preventing them from requiring it and because the average person doesn't read dozens of pages of fine print to make sure a company will not surreptitiously profit off of them. (To check how consumer-friendly a terms and service agreement is before you sign it, Borohovski recommends using the website tosdr.org, which spells out users' rights).

“When was the last time you clicked 'I agree' to these terms and conditions check box and actually read the terms?" Borohovski said. "I do that, most people don’t. A lot of people have kind of given up," trying to protect their data, he said, assuming there is nothing they can do to stay in control of their information. And those people aren't entirely wrong.

A prime example of how this opaque business model serves the financial interests of corporations at the expense of Americans' personal information is 2017’s massive Equifax hack, which exposed the data of nearly 148 million Americans. Most people think of Equifax as a regular credit reporting agency, but it is also a data broker, and that’s the part of their business where they make the most money (and where the data breach actually happened).

"Equifax is more than a credit reporting agency. It's a data broker," Schneier explains on his website. "It collects information about all of us, analyzes it all, and then sells those insights."

"The breadth and depth of information that data brokers have is astonishing," he says. "These brokers collect demographic information: names, addresses, telephone numbers, e-mail addresses, marital status, profession, income level, political affiliation ... they collect lists of things we've purchased, when we've purchased them, and how we paid for them. They keep track of deaths, divorces, and diseases in our families. They collect everything about what we do on the Internet."

Equifax isn't just an average company that provides you, the consumer, with one free credit report a year. It also sells your personal data — including your social security number — to private companies that have nothing to do with credit reports for pure profit, without telling you or asking you. Equifax did not immediately respond to a request for comment.

These companies "deliberately hide their actions and make it difficult for consumers to learn about or control their data," Schneier said. You can try to "opt-out" and tell Equifax that you don’t want your data collected, but it will still collect it anyway — and your data won't actually get deleted, Schneier says.

So what exactly does that mean for consumers? You are the product, not the client. Therefore, Equifax has no incentive to protect your data. Rather, it’s incentivized to serve the banks and retailers that pay it

millions of dollars for the information they have collected on you without your knowledge. These types of companies mitigate the risks of this furtive data brokering by making it a requirement for consumers to agree to their legal terms and conditions, in order to use their services.

Who is safe from this type of data collection?

The short answer: no one. Because there are no laws preventing companies from doing this, you are essentially helpless when it comes to preventing the sale of your own data even if you are meticulous about avoiding entering important information on computers or phones, according to experts.

“Until some innovative company comes along and dis-intermediates these companies, I don’t see anything changing,” said Brian Krebs, a security expert and independent investigative journalist.

And real regulatory changes that would help safeguard people's personal information may not be on the horizon anytime soon. History has shown that companies like Equifax responsible for some of the most egregious recent lapses in corporate responsibility aren't facing many consequences. Even after the breach became public knowledge, the Internal Revenue Service still awarded Equifax with a $7.25 million dollar contract for personal identification services.

"Check back in a year – nothing. And it if they get a fine, it’ll be a fine that was cheaper than the lawyer fees,” Schneier said.

Another potentially worrying aspect of these widespread cyber attacks is the lack of sophistication required to carry them out, experts said. In the case of Equifax, the company would have had to put in minimal effort to secure your data, Bas van Schaik, a researcher at analytics security firm Semmle, told *Wired* in September.

So there's not much I can do to protect my personal information?

Experts told MONEY people can do a few things to have a little more control over their financial information. Specifically, they can freeze their credit reports, get regular copies of their credit report and call to complain when they see something on their report that shouldn't be there.

But ultimately, there is not one action people can take that will prevent companies from collecting their information without their direct knowledge.

Krebs says he's hopeful innovations like blockchain technology will eventually put credit bureaus and data brokers out of business in favor of an approach that gives consumers more control over their financial lives, but he's not holding his breath. For now, Krebs said as long as people continue to check the "I agree to the terms and conditions" box with these companies, data will still continue to be legally collected by every company and service you use.

"I tell people be really careful about the information that you give away whether it’s on social networking on the internet to marketing companies to surveys," Krebs said. "Invariably this information you give away about yourself is used to profile you."

This Search Engine Is Profitable Without Tracking You Online. And Google and Facebook Could Do It Too

By Alix Langone

Facebook could be profitable without tracking you as intently as it does, but the social media network doesn't want you to realize that. Gabriel Weinberg does.

Weinberg is the creator of the search engine DuckDuckGo, an internet privacy company that lets people search the internet without their queries and clicks being tracked. The search engine provides similar search results to Google, though Weinberg says it is still working out some kinks to provide more accurate local results for things like weather and restaurants, as well as breaking news. He started DuckDuckGo almost a decade ago after realizing users had no options to opt out of websites that were tracking their every move on the internet. He self-funded the project for four years before securing a $3 million round of funding led by Union Square Ventures in 2011, the same year TIME named DuckDuckGo one of its 50 Best Websites.

"I saw the trend of advertising and data tracking that was happening at the end of the last decade, and it was getting more pervasive and users didn't really have the option to opt out," he told MONEY. "We thought an alternative option should be available for people."

While DuckDuckGo hasn't permeated our everyday lives like Facebook or [f500link]Google[/f500link] has, Weinberg says the 45-person company's user base is loyal and has been steadily growing. Since its inception, there have been almost 20 billion searches on DuckDuckGo, which is about as many search hits as Google has in four days. But DuckDuckGo has seen its biggest spikes in searches as data tracking continues to be a hot-button issue. The search engine saw daily searches double after Edward Snowden's NSA leaks in 2013. and its traffic jumped 55% in 2017 with daily private queries on its search engine surpassing the 20-million mark.

And the desire for Weinberg's product has only grown in the wake of the Facebook's Cambridge Analytica data privacy scandal, in which almost 90 million users' personal information was improperly collected without their direct consent, forcing CEO Mark Zuckerberg to testify before Congress and leading to a slew of changes to Facebook's privacy settings. In February, before Facebook's data scandal became public, DuckDuckGo saw around 605 million total searches for the month. Once the Facebook revelations came to light, that number spiked to 695 million searches in March and grew to 712 million searches in April.

DuckDuckGo has actively focused on ensuring tracking users' search histories and personal data is not part of their business model. It makes money by showing ads based on search terms for an individual query and affiliate revenue. Many other major companies have done just the opposite. Executives at Facebook, for example, have insisted on numerous occasions that in order to keep the social network free, the way to optimize the company's profitability is by tracking and collecting information about user behavior to serve its data-based advertising model.

But Weinberg says the reality is these companies could still be wildly profitable collecting only a fraction of your information — and cybersecurity experts agree.

"That's an important myth to dispel," he said. "On web search, you really don't need to track anyone to make money because the money is made off of the keyword that you type in." In other words, Google makes money based off of what you type in and search for on Google.com, so its profit comes directly from what word you type in, like "car" or "mortgage," not by keeping track of what other websites you visit and what you click on when you go to those websites.

"Google and Facebook have taken it to a level I don't think people realize," Weinberg said. "They're collecting basically everything about you online because they have hidden trackers on almost every website that's out there." Google deploys hidden trackers on 76% of websites across the web to monitor your behavior in order to make money and Facebook has hidden trackers on about 25% of websites, according to the Princeton Web Transparency & Accountability Project, which monitors and studies how websites collect and use people's data.

Google did not respond to a request for comment for this article, or about its use of hidden trackers. Facebook directed MONEY towards COO Sheryl Sandberg's comments during the company's 2018 Q1 earnings call in which Sandberg reiterated Facebook does not sell user information to advertisers and said users "can opt out of being targeted based on certain information, like the websites you visit or your relationship status."

Those hidden trackers, which follow what you do online even when you're not logged into Facebook or actually Googling something, should be what concerns people most about their online privacy, Weinberg says. But instead, most of the response to Facebook's data privacy scandal involving Cambridge Analytica has focused on changing [f500link ignore=true]Facebook[/f500link] privacy settings and what specific personal data was collected.

Weinberg wants to fight back against the proliferation of hidden trackers, which is why DuckDuckGo recently rolled out a web extension with a built-in tracker blocker. When you're surfing the web, even if you aren't using DuckDuckGo's browser, its web extension automatically blocks hidden trackers on third-party sites, which means companies like Facebook and Google are prevented from tracking you without your knowledge or consent while you're using the internet.

The U.S. is a long way away from enacting any kind of legislation that could help mitigate some of these privacy concerns and help people feel more protected online. But there are some signs of change across the pond. In Europe, privacy protection is top of mind as the General Data Protection Regulation goes into effect at the end of the month. The sweeping data privacy legislation — which is the reason your inbox has been filling up with emails from companies updating their terms of service agreements — is being enacted to limit the power companies have to collect and use consumer's personal data without their consent or knowledge. And Facebook did recently roll out its "Clear History" option, a step in the right direction towards giving consumers greater control over their information, but it still puts the onus on users to protect themselves.

But until there is any substantial law passed in the U.S. akin to the GDPR, protecting your online privacy is going to be tough. Americans will keep finding themselves in the same situation they've experienced over the last few years — waking up to a new story every day about how a company they regularly interact with has had its data compromised or has shared their personal data without their direct knowledge thanks to mandated disclosure, which are the complex agreements written in fine print you have to sign before using the product. Checking the required "I agree to the terms and conditions" boxes is when most people sign away their rights to their personal information without realizing it.

Many people have become more cynical about their ability to protect their privacy online — and experts say they have good reason to be wary. Multiple cybersecurity experts told MONEY that consumers have very few options when it comes to protecting themselves, and that it is up to companies like Facebook and Google to change their business models so that users themselves are not the product being sold.

"[People are] waking up to the fact that their personal information is out there and they want to protect it, but they don't know what to do about it," Weinberg said. "We are trying to set a new standard of trust online. Our mission is to make getting privacy as easy as closing the blinds."

My Cell Phone Number Was Stolen. It Nearly Ruined My Life

By Alix Langone

Megan Clifford was at work when her phone turned off.

Minutes before her phone stopped working on Jan. 8, Clifford received a text message from her cell phone carrier, T-Mobile, saying her online account password was changed and to call the company if she hadn't made the request. When she got a T-Mobile representative on the phone about 30 minutes later to tell them she hadn't made any changes, she was too late. The hackers targeting her had already taken oven her account and transferred her cell phone number to a different carrier.

That was just the beginning of Clifford's month-long struggle to reclaim her identity. While she was still on the phone with T-Mobile, she said she started getting other email alerts: Money from her [f500link]Bank of America[/f500link] and Chase accounts was being transferred to a "name I didn't recognize." That's when she realized the magnitude of her problem: Now that someone had her cell phone number, they could get into her bank account and gain access the common apps she had on her phone, including Venmo and iTunes.

"I realized I had to tell T-Mobile I have to call them back because it was more urgent that I lock up my bank account information," she said.

"You have to change every account, your Spotify — literally everything that's connected to your phone number," Clifford said. "It stops working and you can have to call customer service. I had to pay other fees too because I had no bank account, and payments were hitting and I couldn't pay them. I couldn't even go to the gym."

Clifford, who asked that her age, occupation and hometown not be published due to privacy concerns, is just one victim of an ongoing cell phone "porting" scheme — a scam that all of the major wireless carriers are dealing with, according to Brian Krebs, an investigative journalist and cyber security expert. Hackers use this technique to circumvent two-factor authentication, a popular security measure wherein a randomly generated code is texted to users' phones after they input their password. The problem? Once someone steals your phone number, two-factor authentication can no longer protect you because all of the codes are being sent directly to the hacker.

And while people can practice good password hygiene in an attempt to avoid falling prey to these hackers, personal information can still be jeopardized in other ways, like corporate hacks. In fact, T-Mobile customers may have been more susceptible to the attacks due to a data breach at T-Mobile in 2017 that left many customers' information vulnerable. That security flaw came on the heels of a previous T-Mobile data breach in September 2015, when credit reporting agency Experian was hacked and "an unauthorized party accessed T-Mobile data housed in an Experian server," according to T-Mobile's website.

While exact numbers aren't available on how widespread the unauthorized porting problem is, [f500link]AT&T[/f500link], Sprint, [f500link]Verizon[/f500link] and T-Mobile together established a Mobile Authentication Task Force in late 2017.

A T-Mobile spokesperson said these are industry-wide issues, but did acknowledge a recent "uptick" in cell phone hijacking. T-Mobile representatives told MONEY that the company initially sent a text message earlier this year to millions of its customers about the ongoing scams, and would resend it to customers "who didn't take action the first time." The company declined to discuss any details about customers' experiences or when it first learned of the porting scams.

A community of cell phone porting fraud victims

Dozens of other T-Mobile customers affected by this kind of hack have joined a [f500link]Facebook[/f500link] support group Clifford started called Victims of T-Mobile Porting Identity Theft Scam — six of whom shared similar stories with MONEY about the personal fallout they've dealt with after having their numbers ported without their consent.

For Clifford, her problems multiplied after she learned her cell phone number had been fraudulently ported. When she first called T-Mobile, the representative she spoke with was unaware of the cell phone hijacking scam she was trying to describe. “They had no clue what was going on, even though it happened to many people and they eventually sent a text message about it,” Clifford said. “They didn’t have any policy or procedure to get it fixed right away."

In total, she estimates she lost at least $3,500 from the ordeal — the equivalent of more than a month’s salary for the average American, according to the Bureau of Labor Statistics. The stress and loss of time dealing with the ordeal took a toll, too. Clifford, who is pregnant, described the next month as a blur. She spent the first trimester of her pregnancy in an endless cycle of phone calls with banks and T-Mobile between making trips to the local police station to file fraud claims. Many of those calls were about the $6,000 that was fraudulently transferred out of her account — money that Chase told her she could not get back right away because it was a direct-deposit transfer, not a debit- or credit-card transaction. It took 21 days for the bank to return that money. The bank also froze $14,000 in another one of her accounts, which resulted in her incurring interest and late fees on other bills. None of her direct debit transfers worked either, so bills for utilities like water and trash didn’t go through, and Clifford had to pay fees for voided checks, too.

As with Clifford, a common thread throughout victim's stories is the money was stolen from their bank account using Zelle, a Venmo-like payment app that lets users transfer money instantly, and has recently been adopted by dozens of banks. People who have used Zelle outside of the T-Mobile porting scam have also had money stolen or unauthorized transactions carried on their accounts, in some cases with Zelle refusing to reimburse them, according to personal accounts recounted to MONEY and recent reports from The New York *Times*. Zelle told MONEY "consumers are never liable for unauthorized activity on their accounts. When fraud is reported, or identified, we take immediate steps with our participant banks to investigate and take action, in order to prevent further abuse." Chase spokeswoman Elizabeth Seymour said it is "monitoring this closely," and reimburses customers affected by unauthorized Zelle transactions.

And while Clifford's money was stolen through Chase and Bank of America accounts, a majority of people in Clifford’s Facebook group whose T-Mobile numbers were hacked had [f500link]Wells Fargo[/f500link] bank accounts. John Nowicki, a physician and member of Clifford's Facebook group, said Wells Fargo knew what had happened to his bank account as soon as he walked into his local branch outside of Seattle, Wash. on Jan. 24 to tell them he had been hacked. "It was the bank that told me what happened," he said. "They said, 'You don’t happen to have T-Mobile, do you?' And I said, 'Yeah.' So they said, 'We’ve had this issue where T-Mobile customers have had their number ported and then their money stolen from their bank account.'"

A Wells Fargo representative said the bank is aware of the porting scam and has taken a "number of steps to protect customers," but could not provide specific details about customer's experiences or their policies.

Unfortunately, this experience has become commonplace for the millions of Americans who have been affected by these types of corporate hacks. And security experts recently told MONEY there is not much consumers can to do protect their private information — a startling reality as more major companies like Equifax, Uber and [f500link true=ignore]Yahoo[/f500link] fall victim to hackers.

Two months after her cell-phone hacking nightmare began, Clifford's life has mostly returned back to normal. She and her husband had to freeze their credit and set up credit monitoring. She got back 65,000

points, worth roughly $600, on her credit card. But she never got her cell phone number back. Clifford and other victims say the invasion into their privacy has caused long-term changes in their lives — specifically to how they handle their personal information and the companies who have access to that data.

Ben Malek, who owns his own electronics company based in Tampa, Fla., said after his cell phone number was fraudulently ported out, a credit card was taken out in his name and maxed out in the same day, in addition to money being stolen from both his personal and business bank accounts. He said T-Mobile, which normally sends an email confirming any transactions, ported out his number without notifying him. “Not a single notification,” he said. Just like Clifford, “The only reason I found out is because my phone stopped working.”

His debacle continued to follow a similar pattern as Clifford's. “I got an email from Wells Fargo saying, 'Thank you for contacting us. Please rate the representative that helped you over the phone,” he said. “I called them and said no changes were made. I received an email from Amtrak welcoming me to my upcoming trip to Washington, D.C. — I had no trip planned there. I pretty much thought everything was gone that night.”

Like Clifford, he said many of the T-Mobile representatives he spoke to had no idea what he was talking about when he called to resolve the problem. Once they did, the company still offered no monetary credits or apologies.

And ironically, prior to this incident, Malek said his phone number was one of the only things that made him feel secure, specifically because of two-factor authentication.

"It was very troubling for me," he said. "It’s like you have a security system in your house and then you find out people are able to easily call your security company and say, 'Hey please don’t let the alarm go off,' and they say, 'OK sure no problem.'"

Google Keeps a Record of Your ENTIRE Search History. Here’s How to Delete It in 4 Easy Steps

By Alix Langone

YouTube. Panera. Facebook. Equifax. Every week, it seems, there's a new hack to worry about.

This ever-expanding list has many people realizing their personal information is less secure than they thought. Consumers are looking for ways to limit their online exposure and take proactive measures to protect themselves and their information.

One way to start taking control of your online information is to minimize the ways that advertisers and other companies track and store data they’ve collected on you.

Deleting your Google web browser history and [f500link]Google[/f500link] Google search history is one way to limit how much data you allow to be collected about you on the internet. Even if you're someone who already uses Google's incognito web browser, you're still not being kept completely anonymous online.

Believe it or not, there are other web browsers out there besides Google, they are just much less well-known. One example of a search engine that prioritizes user privacy is DuckDuckGo, which is essentially a Google that doesn't track you online. "It feels like the standard of trust online has really gone down, and we are trying to set a new standard of trust online," said DuckDuckGO's CEO and founder, Gabriel Weinberg. "Our mission is to make getting privacy as easy as closing the blinds."

Even though the push for more transparency online is gaining traction with some newer companies, if you're one of the people making some of the 3.5 billion search queries each day that are processed by Google, chances are you still might want to delete some, or all, of your internet history.

Deleting all of your web browsing activity doesn't get rid of all of the information Google has about you, though. You also have to separately delete certain data like your maps activity if you have "location history" turned on.

Even if you delete all or some of your activity, Google still maintains records data about the way you used its web browser related to the deleted data — if you search for something, it'll still keep a record of the fact that you searched for something at that specific time and date, but not what you specifically you searched for, according to the company's website.

Unlike some other tech companies, Google says it will actually delete the data associated with your account after you completely delete it. Aside from using a web browser like DuckDuckGo, one of the easiest things you can do to ensure your future online activity is not tracked moving forward is too choose "Stop Saving Activity" when you adjust your Google settings.

How to turn off your activity:

1. On your computer, go to Activity controls.
2. Turn off the activity you don't want to save.
3. To confirm, select **Pause**.

Just remember if you delete your history, all of your saved passwords will be wiped too, so you'll have to re-login to all of the sites you had saved passwords for.

Since you've probably already used Google thousands of times in your life at this point, if you want to delete your Google search history and Google browser history, here's how.

How do I delete my Google browser history:

Make sure you're signed into your Google account first (the instructions differ slightly depending on the device you use, but Google has step by step instructions for all kinds of tech).

1. On your computer, open Chrome.
2. At the top right, click More.
3. Click **History.**
4. On the left, click **Clear browsing data**. A box will appear.
5. From the drop-down menu, select how much history you want to delete. To clear everything, select **the beginning of time**.

6. Check the boxes for the info you want Google Chrome to clear, including “browsing history." There are also other types of browsing data you can delete.
7. Click **Clear browsing data**.

How do I delete my Google search history:

1. Go to **"My Activity"** on your computer.
2. At the top right of the page, choose **More --> Delete activity by**.
3. Below **"Delete by date,"** select the **Down arrow --> All time**.
4. Select **Delete**.

If you want to delete only specific items or activity you can also do that in **"My Activity":**

1.
   - Browse by day. At the top right of the page, choose **More --> Item view**
   - Search or use filters.
2. On the item you want to delete, choose **More --> Delete.**

And remember: Even though it's a pain, always read the fine print if you can. And if you need help deciding whether you should really check the "I agree" box on almost any website, you can use the service tosdr.org, which rates companies' terms and services agreements based on how transparent and consumer-friendly they are, so you can make an informed decision.

Google Keeps a Record of Your Entire Chat History. Here's the Trick to Deleting It

By Alix Langone

We've all probably done it—messaged a friend about job drama or something personal while at work.

Numerous studies have found many Americans admit to spending some portion of their work day on personal things like emails and phone calls. A 2015 Findlaw.com survey found 50% of Americans said they used the internet for personal reasons while at work, and a 2014 CareerBuilder survey showed at least one in four workers admitted they spent at least one hour at work on "personal calls, emails or texts."

Chances are high you were hoping to keep at least some of those conversations private. But deleting them, particularly on Google Hangouts (also known as Gchat), is quite complicated. Similar to trying to delete your Google search history, deleting your Google Hangouts history is not as simple as clicking a button.

That's because whoever you're chatting with also has a copy of the chat, meaning they would also need to delete their history to eliminate the conversation's online record.

"When you delete your message history, this is deleted from Gmail and Hangouts on all your devices. Other people in the Hangout can still see the history," Google explains on its help page. Google did not respond to a request for comment on whether Hangouts history is still ultimately stored on [f500link]Google[/f500link] servers.

Follow these steps to delete your Gchat history. If you want to ensure an entire chat history is deleted, make sure you tell whoever you were talking with to also follow these steps:

1. On your computer, go to **Hangouts** at hangouts.google.com or in Gmail.
2. Select a conversation.
3. At the top of the conversation window, click **Settings**.
4. Select **Delete conversation**.
5. If you're sure you want to delete your conversation, click **Delete**.

For deleting messages in group chats, according to Google, you're out of luck. "You can't delete the history for a group, but you can leave the conversation. If someone adds you back to the group conversation, you'll be able to see the history again," according to Google's help page.

You can proactively prevent your Google Hangouts data from being saved moving forward by toggling your conversation history off by following these five easy steps:

1. On your computer, go to **Hangouts** at hangouts.google.com or in Gmail.
2. Open a conversation.
3. At the top, click **Settings**.
4. Check or uncheck "**Conversation history.**"
    - Checked: History is turned on. Messages can be seen in the Hangouts on all your devices and in Gmail.
    - Unchecked: History is turned off. Messages can only be seen for a short time on your devices. Then, the messages won't be saved and will be deleted.
5. Click **Ok**.

However, even with this option there is no guarantee of privacy. Google explicitly notes that network administrators can change this option and that the people you chat with may still have a copy of conversation. "If you use Google through your work or school, your domain administrator can set and change this setting. If you talk to someone who uses a different chat app, their app may keep a separate copy of the conversation's history," Google notes on its site.

How the E.U.'s New Online Privacy Law Could Benefit Users Everywhere

By Alix Langone

It's not just you. Over the past several weeks, many people have been bombarded with emails about data privacy from major corporations such as Twitter and Facebook. There's a reason all these businesses are updating their privacy policies—and, though you may be tempted to trash those emails, they carry news of

real change. The companies sending them have until May 25 to comply with a new privacy law enacted by the European Union, known as the General Data Protection Regulation (GDPR).

What is GDPR compliance?

The E.U. guidelines limit how companies can use and process the personal data of consumers, giving ordinary people more control over their own information. Under the GDPR, corporations need to explicitly ask if they can collect your data, they're required to answer if you inquire what that data is used for, and they must give you the right to permanently delete that information. Companies will also be required to disclose now ubiquitous data breaches within 72 hours.

What will GDPR change?

Even if a company chooses to change its policy for all users, only those covered by the GDPR – so, those in the E.U. – will have legal recourse. But experts say it's still an important reminder for everyone to think about these issues. Many people don't realize just how much businesses rely on data to make determinations about customers. "Your data is being used for significant decisions that are made about you," says Chris Meserole, a fellow at the Brookings Institution. "If you are applying for a credit score, a loan, any number of things, an algorithm can just decide that you're not qualified."

GDPR in the U.S.

As of now, there are no laws in the pipeline to enact similar changes in the U.S., so Americans will have to be satisfied with these secondhand benefits. But the GDPR is already leading some corporations to make changes globally to simplify implementation. If it affects users' attitudes toward privacy the way some experts predict, such changes seem likely to spread.

You've Probably Received a Ton of Privacy Policy Emails This Week. Here's What's Changing

By Alix Langone

If it seems like every tech company—Instagram, Venmo, [f500link]Apple[/f500link], and Twitter, to name a few—has been sending you emails about updated terms of service, you're not imagining it. Hundreds of companies are scrambling to update their data privacy policies ahead of a new European Union law that takes effect on Friday.

And while the new rule — officially known as General Data Protection Regulation (GDPR) — may stem from Europe, its effects are a bit more global. In theory, the GDPR going into effect means it will no longer be acceptable for a business operating in Europe to have a click-to-approve policy that's dozens of scrolls

long and littered with legalese — they will be required to explain their privacy policies in clear and concise ways every ordinary consumer can understand.

That's why even if you live in the U.S., you may be fielding an onslaught of notifications. The new regulations affect not only companies located in the European Union, but also all those that have customers or any sort of operations in an E.U. member country. That includes most of the popular tech companies like Facebook, Twitter and Spotify, as well as many other consumer-facing and non consumer-facing businesses.

https://twitter.com/fart/status/999414307417812992

“U.S. consumers will benefit in a knock-off kind of way,” says Matthew Lewis, head of the Global Regulatory Practice at Axiom Law.

The E.U. isn’t joking around. The GDPR carries hefty penalties in order to ensure compliance. The most egregious offenders could face fines up to 20 million euros, or 4% of their annual revenue—whichever is higher. The 10 biggest tech companies, if found in violation, could accumulate fines that top $50 billion, according to Axiom's research.

"There's a real need [for these companies] to act, which is why you're seeing your inbox fill up," Lewis says.

He added, "This is really prompted by not just giving you more visibility into your data, but more control of it."

Twitter was one of the major companies to roll out a new privacy policy early, announcing the changes in April, saying its new easy-to-understand policy would apply worldwide.

https://twitter.com/Twitter/status/988785567482630144

“We believe you should know the types of data you share with us and how we use it,” the company said on a blog post. "Most importantly, you should have meaningful control over both. We want to empower you to make the best decisions about the information that you share with us and to ensure you feel confident that your data is protected and secure."

The U.S. does not have any such similar laws in place or soon to be in place to protect American consumers. While there are some efforts at the state level to give ordinary consumers more control over their data, such as The California Consumer Privacy Act of 2018, a federal framework for any kind of data privacy regulation is virtually non-existent. It remains to be seen whether the GDPR will prompt the U.S. to take action, but the fact that major companies like Facebook and Spotify are extending their updated privacy policies to protect Americans is a step in the right direction.

These are three of the main changes GDPR requires companies to make:

Consent

Before the GDPR, implied consent was allowed, meaning that companies could add you to their email lists without directly asking you to opt-in, whether you wanted to be on those lists or not.

Now, companies must explicitly gain approval prior to collecting any personal data for anyone in the E.U.— things like name and home address, IP address, location, credit card numbers, age and gender, and more— as well as spelling out what info they're collecting, how they’re storing it, who has access to it, and

how it will be used. Plus, that consent must be easy to withdraw or change. Companies are also required to maintain documentation of your obtained consent.

Had regulation like the GDPR existed before, [f500link]Facebook[/f500link] users in the E.U. would have had legal recourse to pushback against the social media network in the wake of Cambridge Analytica scandal, which led to more than 90 million Facebook users' data being compromised.

Transparency

GDPR also aims to protect consumers even if their data is compromised. Any companies that suffer a data breach must now notify authorities within 72 hours of first becoming aware of it—and notify consumers "without undue delay."

The 72-hour limit would have helped protect consumers in massive data breaches such as Uber's 2016 hack, in which 57 million customers' personal information was stolen. Uber waited more than a year to admit it had been breached, paying the hackers $100,000 to delete the data and keep what happened under wraps.

There's still an open question on whether companies will notify U.S. customers of any breaches, Lewis says. But news travels — so if a company announces a breach in Europe, U.S. consumers will get the message.

Another benefit for consumers? Companies are now also required to employ a data protection officer, a staff expert who can investigate any customer's claim of data misuse or abuse.

Data Portability

Companies must also give users the right to easily access their data, correct it if necessary, and even delete all of it — otherwise known as the right to be forgotten. Companies now have to offer you the option of downloading all of your data, just like Facebook did after the Cambridge Analytica scandal came to a head.

Another right users will now have is the right to anonymity. Companies will be required to randomize their data so individual data sets do not give away which customer is which.