Is it safe?

Understand the issue: Privacy and security

The internet is where we could live, love, learn and communicate freely. To be ourselves, we need to be able to trust the systems that protect us.

A tectonic shift in public awareness about privacy and security in the digital world has occurred in the past year. Some are even calling it "the great privacy awakening."

In 2018, news broke that data analytics firm Cambridge Analytica had harvested data of millions of Facebook users, without their knowledge, and used it for political purposes – including attempts to influence elections in the United Kingdom and the United States.

Public outrage was swift and widespread. Campaigns to make Facebook private by default and to ask users to delete the platform outright took off. Nearly three-quarters of Americans and Canadians reported tightening their Facebook security or distancing themselves from the site altogether. Facebook was grilled in the U.S. Congress and the Canadian House of Commons, fined by the U.K. and sued by the District of Columbia. The company's stock plummeted.

All this was a symptom of a much larger, systemic issue: the dominant business model and currency of today's digital world is based on gathering and selling data about us.

Our datarich digital age have some benefits. Streaming music services recommend songs, based on what we've listened to. Voice recognition technology lowers barriers to access to the internet. City planners have access to more data. Yet, as devices on our streets and in our homes gather more data, a fundamental question remains: Are we too exposed?

Does our awareness extend to making informed choices about commercial DNA tests? Or the privacy settings for apps and online services. We should know the risks of ransomware attacks, why strong passwords are vital and how to judge the security of devices we buy.

We can also support products and services that protect and respect our privacy – like the Tor and Firefox browsers – and demand that other companies do better.

But the responsibility for a healthy internet cannot rest on the shoulders of individuals alone. Just in 2018, millions of people were affected by breaches at Google, Facebook, Quora, Marriott and many others. Over 1 billion Indian citizens were put at risk by a vulnerability in Aadhaar, the government's biometric ID system. Telecommunications providers, including Telus, AT&T and Sprint, were caught selling customers' location data. We need more protection from companies and governments.

There were also bright spots in the last year. Europe's General Data Protection Regulation (GDPR) came into effect, and digital rights organizations are collaborating to ensure it is enforced. Public pressure caused several hackable toys to be pulled off the shelves.

Mark Zuckerberg recently stated that he is committed to "a privacy-focused vision for social networking." But Facebook is also under criminal investigation for data sharing deals with companies including Amazon, Apple, Microsoft and Sony. It's going to take more than words to rebuild the trust that's been lost, not only with Facebook but in the internet overall.

Calls for more privacy regulation are on the rise around the world, some inspired by the idea that companies should treat our data with the same care that a bank would treat our money.

The debate about the dominant business model of the internet – and its implications for the privacy and security of our digital lives – will undoubtedly continue in the years to come. As it does, it's important that we remember the current reality is a human creation, not a technological inevitability. We built this digital world, and we have the power to change it.

23 reasons not to reveal your DNA

DNA testing is a booming global business enabled by the internet. Millions of people have sent samples of their saliva to commercial labs in hopes of learning something new about their personal health or heritage, primarily in the United States and Europe. In some places, commercial tests are banned. In France, you could face a fine of around $ 4,000 USD for taking one.

Industry giants Ancestry.com, 23andMe, MyHeritage and FamilyTreeDNA market their services online, share test results on websites, and even offer tutorials on how to search for relatives in phone directories, or share results in social media. They often also claim rights to your genetic data and sell access to their databases to big pharmaceutical and medtech companies.

In terms of internet health, it's part of a worrying trend of corporations to acquire personal data about people and act in their own best interests, not yours. OK, so test results can also lead to important discoveries about your personal health, and can also be shared for non-profit biomedical research in the public interest. But before you give in to your curiosity, here are 23 reasons not to reveal your DNA – one for each pair of the chromosomes in a human cell.

1. **The results may not be accurate.** Some outputs on personal health and nutrition have been discredited by scientists. One company, Orig3n, misidentified a Labrador Retriever dog's DNA sample as being human in 2018. As Arwa Mahdawi wrote after taking the test, "Nothing I learned was worth the price-tag and privacy risks involved."
2. **Heritage tests are less precise if you don't have European roots.** DNA is analyzed in comparison to samples already on file. Because more people of European descent have taken tests so far, assessments of where your ancestors lived are usually less detailed outside of Europe.
3. **Your DNA says nothing about your culture.** Genetic code can only tell you so much. As Sarah Zhang wrote in 2016, "DNA is not your culture and it certainly isn't guaranteed to tell you anything about the places, history and cultures that shaped you."
4. **Racists are weaponizing the results.** White nationalists have flocked to commercial DNA companies to vie for the highest race-purity points on extremist websites.
5. **DNA tests can't be anonymous.** You could jump through hoops to attempt to mask your name and location, but your DNA is an unique marker of your identity that could be mishandled no matter what.
6. **You will jeopardize the anonymity of family members.** By putting your own DNA in the hands of companies your (known or unknown) relatives could be identifiable to others, possibly against their wishes.
7. **You could become emotionally scarred.** You may discover things you weren't prepared to find out. A fertility watchdog in the United Kingdom called for DNA testing companies to warn consumers of the risks of uncovering traumatic family secrets or disease risks.
8. **Anonymous sperm and egg donors could become a thing of the past.** The likelihood that anonymous donations will remain anonymous decreases with every test taken, which could dissuade donors and negatively affect some families.
9. **Millions are spent on targeted ads to lure you.** DNA companies hand out free kits at sporting events, and create DNA specific music playlists on Spotify. In 2016 alone, Ancestry.com spent $109 million on ads. An ad by AncestryDNA capitalized on "Brexit" and British identity politics, with the slogan, "The average British person's data is 60% European. We may be leaving Europe, but Europe will never leave us."

10. **A pair of socks is a better gift.** You may be tempted by special offers around holidays such as this one, offering 30% off genetic tests for Father's Day: "What do you share with Dad? This Father's Day, celebrate your DNA connection with Dad". Perhaps the man who has everything would prefer not to become your science experiment.
11. **You will become the product.** Your genetic code is valuable. Once you opt in to sharing, you have no idea what company gets access to it, nor for what purpose.
12. **Big pharma wants your DNA.** 23andMe revealed a $300 million USD deal with pharmaceutical giant GlaxoSmithKline in 2018 that gives them access to aggregate customer data. Calico Life Sciences, a medtech company owned by Google's parent company, Alphabet, is the primary research partner of Ancestry.com.
13. **Companies can change their privacy policies.** You might be asked to give your consent again, but policies of companies can still change in ways you may not like.
14. **A company (and your DNA) can change hands.** Companies are bought, sold, go out of business or change their business models. And then what happens with your genetic info?
15. **Destructing your DNA can be difficult.** An investigation into how to delete your DNA from Ancestry.com found that it is possible to erase your record and allegedly even destroy your physical sample. But they don't make it easy.
16. **You have no idea how long they will keep your sample.** Some companies say they keep samples for 1-10 years. Regulations governing DNA databases differ from country to country. Do you know the rules where you live?
17. **Police can access your DNA.** There's crime solving potential, but also human rights risks. Authorities can seek court approval to access consumer DNA databases, but investigators have also been known to create fake profiles using a suspect's DNA.
18. **Your results could become part of a global database.** Law enforcement in several countries have unrestricted access to genetic profiles. Some scientists argue that creating a "universal genetic forensic database" would be the only way to make unwanted intrusion less likely through regulation.

19. **Your data could be hacked, leaked or breached.** Third party sharing is common practice among companies. The more people have access to your DNA, the more vulnerable it is to being hacked. As companies amass more data, they will become increasingly attractive to criminals and vulnerable to cyber theft.
20. **Genes can be hacked.** Scientists have discovered how to store data and even animated GIFs in DNA, and even believe malware could be placed in DNA to compromise the security of computers holding databases. Still trust them?
21. **You are signing away rights.** When you use services like AncestryDNA the default agreement is to let them transfer your genetic information to others, royalty-free, for product development, personalized product offers, research and more.
22. **Companies profit from your DNA.** Testing isn't the only way companies make money. They profit from data sharing agreements with research institutes and the pharmaceutical industry. If your DNA helps develop a cure for a disease, you'll never know. And you certainly won't earn royalties from any related drug sales.
23. **You may be discriminated against in the future.** In the United States, health insurers and workplaces are not allowed to discriminate based on DNA. But the law does not apply to life insurance or disability insurance. Who knows in your case, where you live? Some day you could be compelled to share genetic information with your own insurer.

If you still decide to submit your DNA for testing, the U.S. Federal Trade Commission offers sound advice to consumers: compare privacy policies before you pick a company, choose your account options carefully, recognize the risks, and report any concerns to authorities. To counteract the dominance of commercial companies, you can also contribute your data to nonprofit research repositories like All of Us or DNA.Land that are open to public scrutiny.

If you regret a choice you made in the past, you could have your DNA data deleted and request that your sample be destroyed. Consumer DNA testing is an example of why strong data protection laws are so important. In Europe, the General Data Protection Regulation (GDPR) offers some protections, but elsewhere you have few rights when you hand over sensitive data.

► Further reading

- How DNA Testing Botched My Family's Heritage, and Probably Yours, Too, Gizmodo, 2018. https://gizmodo.com/how-dna-testing-botched-my-families-heritage-and-probab-1820932637
- Ancestry wants your spit, your DNA and your trust. Should you give them all three?, McClatchy, 2018. https://www.mcclatchydc.com/news/nation-world/article210692689.html
- The Forensic Genetics Policy Initiative – Country Wiki. http://dnapolicyinitiative.org/wiki/index.php?title=Main_Page

In defense of anonymity

When bad things happen over the internet, anonymity often gets the blame.

It may seem logical to think that if we could identify each and every person online, we could prevent crime. In every part of the world, there are authorities who argue that encryption should be banned or that anonymous sites should be eradicated. The reality is that anonymity often protects victims of crime, in a wide range of areas, from human rights, to banking security, military defense, or personal safety from stalking and domestic violence.

Constant surveillance facilitated by digital technology, whether by corporations or governments, is harmful to society and chilling to civil liberties. Our ability to communicate, work, and learn on the internet free from the glare of others enables very good things to happen.

Being untraceable on the internet takes effort. For that, Tor is one of the most important anonymity and censorship circumvention tools. An estimated 2 million daily users use it to hide the origin and destination of internet traffic as they browse the Web and communicate around the world.

In the context of concerns over terror and crime on the internet, Tor is often vilified. In the daily position of defending anonymity is *Stephanie Ann Whited*, the communications director of the Tor Project.

Q: What are questions you get from journalists that frustrate you?

Stephanie Ann Whited: It's frustrating to be asked questions based on the misunderstanding that Tor "is the dark web."

Tor onion services can be used to publish and share information online with a high degree of privacy and security without being indexed by search engines. You can't just visit them in any browser. Calling this "the dark web" and assuming everything published anonymously online is bad, is a huge disservice to an underappreciated technology that saves lives.

With onion services, women can share and access women's health resources in countries where it is outlawed. Activists can organize with less fear of surveillance when there may be life or death consequences. Whistleblowers reporting corruption can communicate securely. Onion services have also been used to create a more secure way to access popular sites like The New York Times, Facebook, or ProPublica. They all have .onion addresses.

Q: What makes your work feel most meaningful?

Internet freedom is in decline around the world, and being part of a force for good that allows people to have private access to the open Web is hugely important to me. Millions of people around the world rely on Tor Browser and onion services for private and secure communication in their day-to-day lives.

Some people rightly just want to limit the amount of data big corporations and advertisers can collect about them. For others, Tor is a vital tool against government oppression.

During protests in Sudan this year, when social media was blocked, Tor Browser usage spiked. It's also actively used in Uganda where a tax on social media was introduced.

Q: When you hear about the serious crimes that really do happen on onion sites (the so-called "darknet") does it make you doubt your sense of purpose?

It can be upsetting to hear Tor was used in a serious crime, but it doesn't make me doubt the software or the good that is only possible with anonymity tools like Tor. The reality is that criminal activity exists on all kinds of sites, whether they were configured using onion services or not. Getting rid of Tor, or even getting rid of the internet, wouldn't make crime go away.

Q: Has press coverage about Tor changed over time?

Yes, and I think it's because we've improved the consistency and frequency of our communications and made Tor more user-friendly. Also, a lot more people are coming to understand how their daily online activities are exploited by tech giants. Even when other browsers offer more privacy protections than they used to, the full benefits of Tor Browser are unmatched. The press is beginning to highlight that more often without caveats.

Q: What are exciting things that are happening in the world of Tor?

Tor is more user-friendly and faster than ever. A decentralized network of over 7,000 volunteer-run servers around the world make up the backbone of our software, and we just surpassed over 40 GiB/s total bandwidth thanks to our community of volunteer relay operators.

The release of our first official mobile browser, Tor Browser for Android in 2018, is enabling us to reach more people in the parts of the world that need Tor most.

► Further reading

- Tor Metrics. https://metrics.torproject.org/
- "Tor is easier than ever. Time to give it a try", WIRED, January 2019. https://www.wired.com/story/tor-anonymity-easier-than-ever/
- If anonymity isn't the problem, what is?, Internet Health Report, 2018. https://internethealthreport.org/2018/if-anonymity-isnt-the-problem-what-is/

Ransomware payments add up

We don't know who is making the payments, or who is receiving them. But by looking at the public protocols of Bitcoin accounts associated with ransomware we can see the trail of money paid.

How much would you pay to regain access to your computer files? This is a question victims of ransomware are faced with when they least expect it. A threatening message appears promising to delete all files unless a payment is made before a certain time.

"My first reaction was panic. My second reaction was to get on another computer and figure out exactly how much 1.71 Bitcoin was worth in US dollars," said John, a lawyer in Chicago, describing a ransomware attack that temporarily crippled his legal practice in 2016.

A malicious link clicked or a file attachment arriving by email can unleash ransomware on networked computers or mobile phones. It can take down healthcare providers and threaten the aviation industry. Estimates of how many people and companies are affected by ransomware vary, but it's a big crime business. Software to unleash an attack can be easily bought and customized. Network security company SonicWall counted more than 200 million attacks globally in 2018. Cisco estimates that every 40 seconds a business falls victim.

In recent years, international law enforcement and security firms have collaborated on The No More Ransom Initiative to freely share decryption tools. This has helped people worldwide. Creating frequent backups of files and keeping operating system software updated is the best fix to keeping your own devices healthy and free of malware that can infect others too.

Secrecy clouds what we know about the economic impact of ransomware.

A 2018 study about ransomware payments via Bitcoin, "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective" offers a glimpse of how many people fall prey, and suggests a new counting method to better estimate the millions of dollars of payments. For instance, on May 15, 2017 alone the equivalent of $ 24,246.51 USD in ransom payments were transferred to WannaCry ransomware attackers [see animated data visualization on the Internet Health Report 2019 website]. In few days, an estimated 300,000 businesses in 150 countries were hit. There are still new WannaCry victims today.

► Further reading

- The No More Ransom Initiative. https://www.nomoreransom.org/
- On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective; Mauro Conti, Ankit Gangwal and Sushmita Ruj, 2018. https://arxiv.org/abs/1804.01341
- With Ransomware, It's Pay and Embolden Perpetrators, or Lose Precious Data, The New York Times, May 2017. https://www.nytimes.com/2017/05/17/technology/bitcoin-ransomware-pay-lose-data.html

Coordinating complaints for data privacy in Europe

Civil society organisations in Europe are playing a crucial role in enhancing the effectiveness of the European General Data Protection Regulation (GDPR) by using its enforcement provisions to challenge established practices of some of the biggest technology companies in the world.

The GDPR addresses some of the power imbalances between users and tech companies that operate globally. It has strengthened existing rules and given new powers to enforcement authorities. Companies and organizations are forced to be more transparent about how they collect and process personal data.

Even though the GDPR is a European regulation, it is relevant globally. First, because it applies to data collection about European citizens, it is recognized by many internet companies that dominate the global web. Second, countries around the world are watching to understand its strengths and weaknesses as they consider similar regulations.

One year since the law came into effect in May 2018, the efforts of filing complaints across Europe are beginning to bear fruit. By helping users going after companies that collect their data, digital rights organizations in Europe hope to improve how privacy regulations are being enforced to close the gap between legal protections and actual practice.

In January 2019, Google was fined €50 million Euros (about $57 million USD) by the national Data Protection Authority (CNIL) in France following two complaints on "forced consent" by noyb – European Center for Digital Rights in Austria and La Quadrature du Net in France.

Is GDPR working?

A coalition of digital rights organizations in Europe have created the publication GDPR Today to collaboratively collect and publish statistics that help advocacy organizations across Europe understand how the GDPR is being applied and to raise awareness of EU rights.

There are inconsistencies in how different countries collect and provide data but GDPR Today has compiled reports of data breaches and complaints from 10 out of 28 European Union countries in their March 2019 edition.

Between May 2018 and March 2019, there have been at least 71,237 complaints and 28,977 data breach notifications reported in those ten countries

alone – all varying in nature. The Irish data protection authority reports that among the 1,928 GDPR complaints they received between May and December 2018, most fall under the categories of "Access Requests" (30 %), closely followed by "Unfair Processing of Data" (15 %) and "Disclosure" (11 %).

An important right granted by the GDPR is that individuals can request a copy of the data collected about themselves in an unedited and intelligible form. This allows individuals and watchdog organizations to get a better sense of what personal data online services collect. noyb has tested whether and how popular streaming services comply with this requirement by requesting a copy of user data from a variety of companies. According to noyb, none were fully compliant. They filed ten different complaints against eight streaming services in January 2019.

Other contributors to GDPR Today have similarly filed complaints to advocate for a better enforcement of existing protections including Panoptykon, Privacy International and Open Rights Group.

It's clear, the GDPR will only be as effective as its enforcement, and civil society groups are playing a crucial role in ensuring that enforcement happens. That is an important lesson not only for Europe, but for privacy advocates around the world. As data protection authorities across Europe react to these complaints we will see what effect GDPR ultimately has.

► Further reading

- How Is the GDPR Doing?, Slate, 2019. https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html
- GDPR explained, Bits of Freedom, European Digital Rights (EDRi) and Panoptykon Foundation, 2018. https://gdprexplained.eu/

Your mobile apps are tracking you

If you have any apps installed on your mobile phone – be it games, news or fitness apps – it's likely that you are sending some kind of data about your identity, preferences, or physical location to Google, Facebook and other companies without even knowing. This alone shouldn't be news to you, but new research now documents how significant the issue is in scale.

An Oxford University study of nearly 1 million free Android apps in 2018 revealed that the majority of mobile apps contain utilities from companies – including Alphabet, Facebook, Twitter, Verizon, Microsoft and Amazon – that enable them to track and send data about users to these companies. These utilities are incorporated by app developers for a variety of reasons. For instance, the app developer might use them to monitor the use of the app or to display ads.

The researchers make no claims about what data is transferred to companies, but warn that it's common for them to gain access to data that is not directly related to the app in use. Depending on app permissions, this could be as broad as a contact list or location history.

With transparency lacking about what is tracked by whom, the researchers see potential privacy risks that leave people vulnerable. Data combined from multiple apps, along with other online history and behavior, can be used to generate very detailed profiles of individuals. From the apps on a person's phone you could estimate interests, sexual orientation, health status and the identities of their children.

Google disputed the negative implications of the study, telling the Financial Times in October that the researchers mischaracterize "ordinary functions" such as an app merely sending a crash report. Reuben Binns, the computer scientist who led the study, says, "Nobody has disputed that the third parties we identify in the study are capable of tracking user behaviour across multiple apps. This includes when data is used for analytics, crash reporting or – as in 60% of apps with Google's DoubleClick tracker embedded – behaviourally targeted advertising."

On the Web, trackers can log information about what you search, click and type. A variety of browser tools (like Privacy Badger, Ghostery or Lightbeam) exist to see who is tracking you. You can also block access to third party trackers or tracking cookies (see Brave or Firefox, Chrome or Safari) though this usually also means blocking ads because they have the capability to track.

On mobiles, users can turn off or reset advertising identifiers that track them across apps, similar to blocking cookies on the Web. But since many users have no idea this tracking is occurring across apps, they also don't know they can take control.

In the case of Google, they control what apps are available in the Google Play Store for the Android operating system *and* also benefit from the data

generated by those apps. The Oxford University study found that Alphabet is the ultimate owner of several subsidiaries that together were found to have trackers in more than 88 % of the analyzed apps.

New research on smartphones sold by more than 200 different vendors points to an additional risk of invasive data collection with some apps that are pre-installed by manufacturers. "Users are clueless about the various data-sharing relationships and partnerships that exist between companies that have a hand in deciding what comes pre-installed on their phones," says the study, while calling for more transparency and real opportunity for consent about data collection.

Privacy protections *could* be built into phones from the start, but they are not. With an app ecosystem that is designed for maximum data collection behind the scenes we should not be surprised. As more of us wake up to privacy risks online, we also need to recognize the privacy risks of the smartphones that are now so important to our lives. Knowing is half the battle.

► Further reading

- AppCensus. https://www.appcensus.io/
- Third Party Tracking in the Mobile Ecosystem by Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt, Proceedings of the 10th ACM Conference on Web Science, 2018. https://arxiv.org/abs/1804.03603
- Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, The New York Times, December, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html
- An Analysis of Pre-installed Android Software, Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador and Narseo Vallina-Rodriguez, 2019. https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf