End-To-End Encryption

What are you hiding?

By David Bruno – Spring 2020

Abstract

Social interactions are contextual. People wouldn’t necessarily admit to certain beliefs or divulge personal secrets to a random stranger the way they would confide in their partner. Yet, this seemingly natural right breaks down completely in the digital world.

The tendency to abandon private data for free online interactions has fuelled the rise of surveillance capitalism and digital authoritarianism.

A subset of users who understand this threat and are attempting to safeguard their data have adopted end-to-end encryption as their tool of choice.

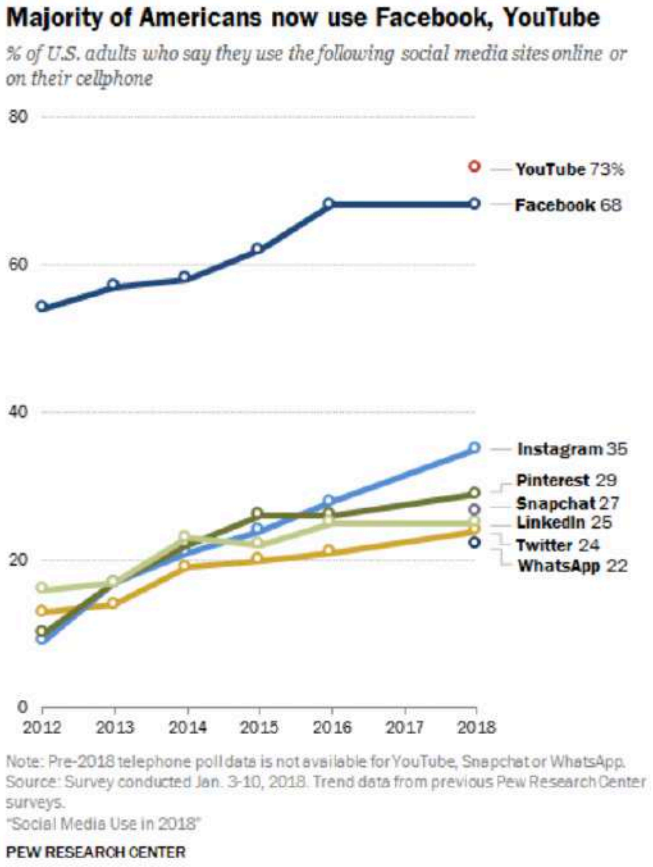
Introduction

So many of our interactions are contextual. People wouldn't necessarily admit to certain beliefs or divulge personal secrets to a random stranger the way they would confide in their partner. Most would probably talk to their friends about subjects they would never discuss with their parents.

It's not that certain thoughts or ideas are nefarious or deviant. It's just that people exercise a right to control the flow of their personal information.

Yet, this seemingly natural right breaks down completely in the digital world. A Pew Research study from 2016 found that 49% of people would be okay sharing personal information with a free social media site. In practice, of course, we know that people are a lot more liberal with their personal data. 68% of adults in the U.S. use Facebook, while roughly 2 billion use the platform across the world.

From Google to TikTok, digital behemoths have built hundreds of billions of dollars in value through leveraging personal data given away for free or extremely cheaply. Data's value, it appears is a lot lower when it's packaged in likes and retweets across the digital world. In fact, creators of this digital landscape are critical of any effort to protect private information online.
The argument was clearly described by Google CEO Eric Schmidt, when he said: "If you're doing something you don't want anyone to know, maybe you shouldn't be doing it in the first place."



Majority of Americans now use Facebook, YouTube

% of U.S. adults who say they use the following social media sites online or on their cellphone

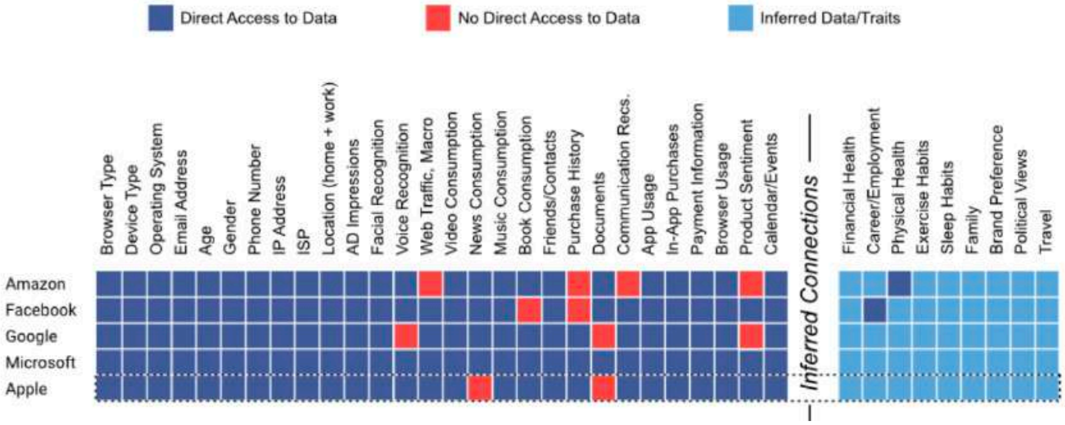
Note: Pre-2018 telephone poll data is not available for YouTube, Snapchat or WhatsApp.
Source: Survey conducted Jan. 3-10, 2018. Trend data from previous Pew Research Center surveys.
"Social Media Use in 2018"
PEW RESEARCH CENTER

Source: Pew Research Centre

The nothing-to-hide argument lives on today, even after several high-profile incidents of data loss and nefarious abuses. In this paper, we explore the current landscape of data-driven digital technologies, the social and political impact of our tech-driven surveillance state and the tools available for those looking to safeguard their data in an info-hungry world.

Rise of the surveillance economy

"I define surveillance capitalism as the unilateral claiming of private human experience as free raw material for translation into behavioral data. These data are then computed and packaged as prediction products and sold into behavioral futures markets — business customers with a commercial interest in knowing what we will do now, soon, and later," says Shoshana Zuboff, professor emerita at Harvard Business School, who wrote a book on the subject. Professor Zuboff believes Google was the first company to recognize the value of data and leverage it in this way. Later, platforms like Facebook, Twitter and TikTok emerged to use the same business model to create multi-billion dollar companies. Some of the richest people in the tech industry have built their fortune on the wholesale capture and use of personal information.



■ Direct Access to Data 🟥 No Direct Access to Data 🟦 Inferred Data/Traits

	Browser Type	Device Type	Operating System	Email Address	Age	Gender	Phone Number	IP Address	ISP	Location (home + work)	AD Impressions	Facial Recognition	Voice Recognition	Web Traffic, Macro	Video Consumption	News Consumption	Music Consumption	Book Consumption	Friends/Contacts	Purchase History	Documents	Communication Recs.	App Usage	In-App Purchases	Payment Information	Browser Usage	Product Sentiment	Calendar/Events
Amazon	■	■	■	■	■	■	■	■	■	■	■	■	■	🟥	■	■	■	■	■	🟥	■	🟥	■	■	■	■	🟥	■
Facebook	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	🟥	■	🟥	■	■	■	■	■	■	■	■
Google	■	■	■	■	■	■	■	■	■	■	■	■	🟥	■	■	■	■	■	■	■	🟥	■	■	■	■	■	🟥	■
Microsoft	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Apple	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	🟥	■	■	■	■	🟥	■	■	■	■	■	■	■

	Financial Health	Career/Employment	Physical Health	Exercise Habits	Sleep Habits	Family	Brand Preference	Political Views	Travel
Amazon	🟦	🟦	■	🟦	🟦	🟦	🟦	🟦	🟦
Facebook	🟦	■	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Google	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Microsoft	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Apple	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

Source: HowDo

This surveillance capitalism seems to have distorted public discourse and reshaped the economy with regrettable effects. Journalistic institutions are no longer considered trustworthy and are driven to create "click-worthy content" rather than hold institutions accountable and investigate malpractice.

Incumbent tech giants can crush smaller players and domestic competitors in countries they enter simply because they have all the relevant data. Deeply private information is being shared with lawyers and pharmaceutical companies to fuel the modern economy at the expense of basic privacy.

However, the abuse of data becomes a lot more sinister when it transitions from commercial to political applications. A few recent examples paint a disturbing state of affairs across the globe:

- North Korea uses sophisticated spyware and malware tools to infiltrate foreign companies and steal vital intellectual property or commit insurance fraud to generate revenue for the regime.
- Consulting firm Cambridge Analytica harvested the personal information of more than fifty million Facebook users and offered it to clients, including the Trump campaign, sabotaging the democratic process in America.
- China's use of Credit Scoring, the Great Fire Wall and facial recognition has been used to crack down on public dissent and detain millions of ethnic Uighurs.
- Iranian security services reportedly worked with counterparts in China to import facial recognition software that is being used to crack down on protestors and dissenters across the nation.

Source: Wired

Several other cases highlight the grievous impact this loss of digital data and privacy has had on oppressed citizens under both authoritarian and flawed democratic regimes. It should be clear that the right to privacy is as vital as the right to free speech or right to freedom, because privacy underpins those other rights.

Leaders of the Free World Abandon Privacy

While a lack of privacy and rise in surveillance could be expected in countries under authoritarian regimes, the bigger concern seems to be the rise of this trend in the so-called "free world." The growing number of attacks on digital encryption and data privacy in the United States of America are particularly egregious.

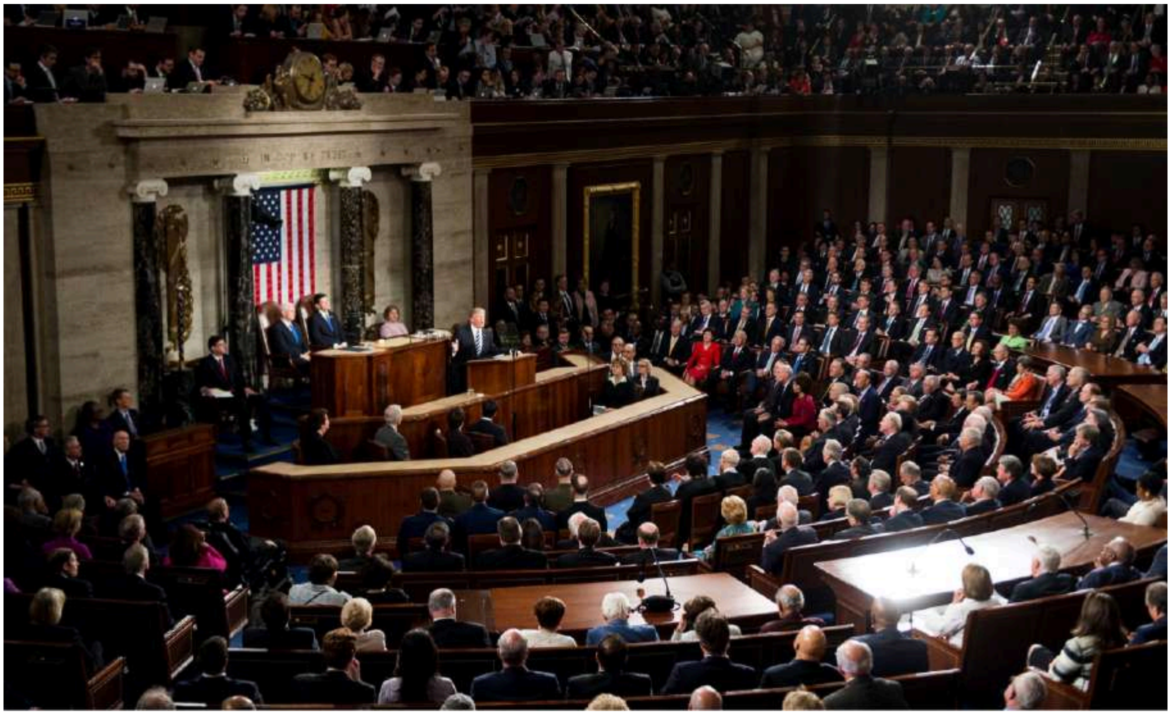
U.S. Senators Lindsey Graham and Richard Blumenthal recently introduced a proposal that would give the Attorney General the power to unilaterally write new rules for how online platforms and services must operate in order to rely on Section 230. Section 230 limits liability for tech companies with regard to how their users use the platforms. Under the new proposal, the tech companies would have to "earn" this protection by demonstrating that they are following the recommendations set by a 16-person commission.

The proposal, known as the "Eliminating Abusive and Rampant Neglect of Interactive Technologies" or EARN IT Act, was described as "a sneak attack on encryption." It imperils tech companies and opens a gateway into private communications online that can be easily accessed by authorities. While the proposal is officially aimed at clamping down on child abuse and exploitation, critics say the new rules would give the AG too much power over citizens' digital lives.

This isn't the first time Republican legislators have expressed their disdain for encryption and online privacy. Back in 2016, during the presidential campaign, candidate Jeb Bush said encryption, "makes it harder for the American government to do its job," while his rival Carly Fiorina said tech companies must "tear down cyberwalls."

President Donald Trump, of course, isn't keen on encryption either. The administration is actively considering legislation prohibiting tech companies from using forms of encryption that law enforcement can't break.

The President also asked Apple to consider weakening its encryption after the company refused to create backdoors that would make it easier to unlock iPhones.



Source: Flickr

It isn't just the legislators involved in weakening privacy. Earlier this year, The Swiss government has ordered an inquiry into a global encryption company based in Zug following revelations it was owned and controlled for decades by US and German intelligence, indicating that American intelligence agencies were also involved in weakening data protection across the world.

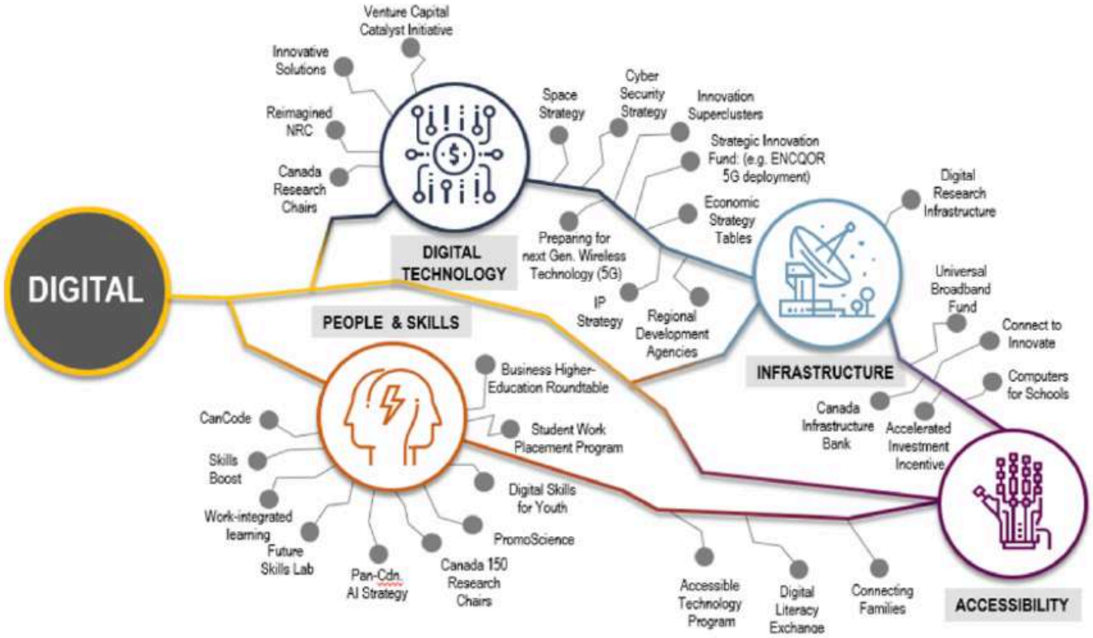
These aggressive clampdowns on technology companies and digital platforms could weaken the U.S.'s position on the Global Privacy Index, which is currently hovering around 68.6.

By comparison, other parts of the world are much higher on the index due to their decisive actions in protecting online data. The European Commission officials confirmed last year that they would not consider a ban on encryption in the region and pointing out that the General Data Protection Regulation (GDPR) explicitly refers to encryption as a privacy protection measure. Eurozone countries such as Norway, Sweden and Denmark are at the top of the Global Privacy Index.

Canada also ranks higher than the U.S. on the Global Privacy Index. The country has a privacy score of 81.8, placing it at 7th position on the index just behind Germany.

Canadian authorities have taken decisive steps in recent years to bolster online privacy further.

Last year, the Honourable Navdeep Bains, Minister of Innovation, Science and Economic Development, launched Canada's new Digital Charter. The Charter sets out ten principles, ranging from "a level playing field for all users" to "a commitment to digital governance" and "Universal Access" to digital technologies.



Source: Flickr

The government has also implemented the CyberSecure Canada program last year that certifies small and midsize businesses based on their ability to meet minimum standards for data protection and online privacy. These actions are regarded as a major step forward by advocates of digital privacy.

However, Canada and the European Union are rare exceptions. The global trend seems to be heading towards weaker encryption and stronger authoritarianism and surveillance in the digital world.

Data protection and privacy rights are under attack across the world and have compelled privacy advocates and a handful of corporations to adopt new

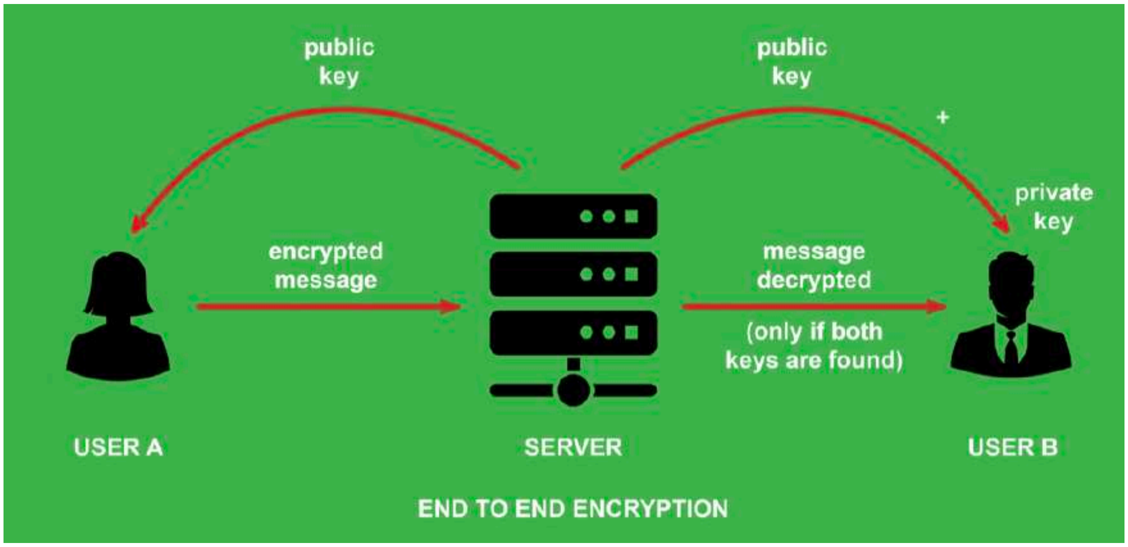
tools that can safeguard digital communications and data.

The solution

The most effective tool in the fight to safeguard privacy is end-to-end encryption (E2EE).

As the name suggests, E2EE is a system of digital communications that restricts messages and data to only two ends: sender and receiver. Effectively, E2EE should keep all third parties - including telecom providers, rogue government intelligence agencies, internet providers, and even the provider of the communication service - out of the private messages of users.

The first free, widely used end-to-end encrypted messaging software was PGP, or Pretty Good Privacy, a program coded by Phil Zimmermann and released in 1991. Decades later, the cryptographic that secures messages and the technology needed to implement E2EE in consumer tech platforms has become more commonplace.



Source: GeeksforGeeks

However, in practice some corporations retain the private encryption keys that secure the messages in the first place, effectively diminishing the promise of E2EE. Meanwhile, some corporations have been pushed away from adopting E2EE after facing pressure from government authorities. Apple, for example, ditched its plan to adopt E2EE for iCloud in 2018 after facing pressure from the FBI.

The U.S. Congress went a step further and introduced the EARN IT Act of 2019, which would make it much more difficult for corporations to adopt E2EE for their customers and users.

This backlash from government agencies and authorities should make it clear: E2EE is effective when deployed properly. Platforms with E2EE built in and corporations based in privacy-conscious jurisdiction such as Switzerland could help the average internet user protect her privacy and take control of her personal data.

Readily available and time-tested E2EE platforms could be the final barrier between libertarian democracy and an authoritarian dystopia.

Bottom line

To understand the privacy debate, replace the question “what do you have to hide?” with “what do you have to lose?” With the rise of surveillance capitalism and data-driven authoritarianism, the answer is clear: “liberty and freedom.”

The ability to control private data and information is a fundamental human right, on par with the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression. By adopting end-to-end encryption tools, users across the world can finally reclaim this fundamental right.

Bottom line

As founder and CEO of a global cyber security firm, David specialises in anti-fraud and anti-corporate espionage systems for banks and financial institutions worldwide. Through his company, Secure Swiss Data (now SafeSwiss®),
he provides financial sector solutions for the digital, interactive and FinTech sectors. For 20 years he has worked to
provide security protections to the masses and has invested his own money in a free encrypted email server for the
public. He educates on the surveillance of email in general and the importance of encryption, especially for vulnerable

About David Bruno

As founder and CEO of a global cyber security firm, David specialises in anti-fraud and anti-corporate espionage systems for banks and financial institutions worldwide. Through his company, Secure Swiss Data (now SafeSwiss®), he provides financial sector solutions for the digital, interactive and FinTech sectors. For 20 years he has worked to provide security protections to the masses and has invested his own money in a free encrypted email server for the public. He educates on the surveillance of email in general and the importance of encryption, especially for vulnerable populations like refugees.