DATA AND PRIVACY, OPINIONS, TRENDS

Privacy is dead. Long live privacy!

ART BY Chris Koehler

Almost every new technology is said to have finally killed privacy. One thing's for sure: Regulation alone can't keep our personal data safe.

5 minute read

AUTHOR
Sherry Jones

SHARE ARTICLE

Every year news headlines warn a new technology means privacy is gasping its final breath. But doomsday scenarios predicting privacy's death are nearly as old as the notion of privacy itself – which, it turns out, isn't that old. In this article, I'll explore western society's relationship to privacy through the years, and the implications for us all in the digital age.

Dreaming of privacy from a communal bed

The idea of privacy began in 19th-century England, writes Georges Duby in the series, A history of private life. The word "privacy" came from the French *priver* – to tame or domesticate. The classical Latin *privatum,* similarly, refers to what happens in the home or within the family circle.

In the Middle Ages, Duby maintains, time alone was a rare commodity. Beds were prohibitively expensive. All but the wealthiest families shared one. And although royalty and aristocrats might have had their own beds, their bedrooms were hardly solitary. Servants and guards always remained at hand.

Sharing sleeping quarters wasn't unique to western societies. Anthropologists studying the Trobriand Islanders, an ancient hunter-gatherer culture living off the coast of New Guinea, reported families lived and slept in one-room huts. When the parents wanted to be intimate, they told their children to cover their heads with mats.

Having an ale, and someone else's mail

Privacy in mail delivery was also once spotty. Even a wax seal didn't guarantee an envelope would arrive unopened, its contents unread.

In The right to privacy in American history, David J Seipp describes how in the 19th century, letters from England arrived on merchant ships.

These letters were delivered to taverns, then lay in a mailbag available to all, until claimed by addressees – or anyone else.

The British government's Post Office Act established an official postal service in America in 1710 forbade opening someone else's mail, becoming the United States' first privacy law.

By establishing a postal service, the government aimed to protect individuals' privacy. But not everyone used it. Some preferred the convenience of merchant ship delivery, despite its risks.

When telephones came to the party

Likewise, when the first telephones appeared in the US, some predicted this new technology would be personal privacy's death knell. They had good reason. The earliest phones were in public locales like general stores. People heard everyone else's calls while they lined up to make and receive their own. Calls went through a central switchboard, where operators made manual connections while overhearing conversations.

When phones became common in the home, many were on "party lines" – several households sharing one line. When someone wanted to make a call, they picked up the receiver and checked for a dial tone. If others were using the line, the caller heard their conversation.

Despite concerns about privacy, people kept using the telephone. It let them share information in real-time rather than sending costly telegrams or letters that took days, weeks or months to arrive.

Perhaps people were willing to sacrifice some privacy because they trusted technology could solve the problems it created. In time, private phone lines became increasingly available, and party lines disappeared.

Hackable yet desirable

The digital age has presented its own set of privacy challenges. An internet designed to facilitate the free and open exchange of information is also one that lets information be used in ways we don't always like.

Governments conduct "digital surveillance" of citizens using facial recognition technology. Digital personal assistants – such as Amazon's Alexa and Apple's Siri, "smart" television sets, and other internet-connected home devices have been hacked. Yet sales of internet of things (IoT) devices keep rising. One report predicts the number of voice assistants in use will more than triple by 2023, to eight billion.

Protecting us from ourselves

Some might say privacy is already taking a back seat to the convenience the internet affords. At the same time, people and organizations clamor for ever-more-stringent personal data protection.

Governments globally are beginning to impose strict controls over the collection, use, sharing and sale of personal data. Most notable are the European Union's General Data Protection Regulation (GDPR) and the US State of California's California Consumer Privacy Act (CCPA).

While governments step up privacy protection, people keep posting their personal details online.

Many freely give up private information without knowing how it will be used. Privacy watchdogs and consumers worldwide are increasingly concerned about the potential use of "big tech" – including Google, Facebook and Apple – for political and cultural manipulation.

The US Federal Trade Commission fined social media site Facebook five billion US dollars for selling users' data to political consultancy Cambridge Analytica. Recent news reports indicate Cambridge Analytica used social media to influence political elections around the world.

Big brother is watching, but do consumers care?

Does personal privacy matter to consumers today, or doesn't it? The answer may depend on who we ask.

Millennials supposedly have a devil-may-care attitude about the security of their personal information. In a 2016 US and UK study, seventy percent of millennials (aged 19 to 36) said they think their online privacy will probably be compromised and were *not* alarmed. But more recently, the Internet Innovation Alliance found no significant difference between generations on data privacy concerns.

In a 2019 Internet Society survey of consumers in Australia, Canada, Japan, France, the UK and the US, 75 percent expressed concern about companies sharing their personal data without their permission. Even more – 88 percent – want governments to guarantee their right to data privacy, while 80 percent thought laws and regulations are not enough.

And they're right.

Innovations that aim to protect privacy

History shows us technology and human ingenuity can often solve the problems they create.

When people post their personal information on social media, they're choosing to do so. The violation occurs when a social media or other site sells or shares that information without its owner's consent. But an open and freely accessible internet doesn't have to mean exposing our most sensitive data.

Laws can help protect us, but they can only go so far. And lawmakers are still grappling with how best to impose restrictions on data collection and use without hindering free enterprise.

The light at the end of the privacy tunnel is innovation. In response to increasing concerns over personal data collection and use, technology companies are starting to give internet users alternatives – to choose privacy, or not.

The DuckDuckGo search engine doesn't save users' search history, nor share their data. Some adblockers provide a similar service.

The social media site MeWe gives users a Privacy Bill of Rights, promising data belongs only to the user and the site will never sell or share it.

For businesses, tech startup Duality Technologies invented 'homomorphic encryption,' letting technology companies analyze encrypted personal data without unencrypting it. Reportedly, Google now provides a homomorphic encryption tool to its business partners.

Emerging technologies also hold promise for improving privacy.

Blockchain, the basis of Bitcoin and other digital currencies, links transactions in a "distributed ledger," visible to users and unchangeable. Some predict Blockchain will be another means of creating encrypted digital identities.

One startup, Polys, is using encryption and Blockchain together to make online voting both anonymous, protecting voters' privacy, and verifiable, ensuring the security of results.

Admittedly, some who design technologies and run companies may not have public interests at heart. Laws are needed, therefore, to safeguard privacy. But even consumers recognize governments can't do it all.

The dawn of a new privacy era: What businesses should do

In the fight for data privacy, we need tighter regulation. But if too heavy-handed, legal restrictions could hinder innovation.

The best remedy is a combination of the two: flexible privacy laws plus digital offerings that enable users to protect their data. This "one-two punch" will usher in a new age in which our information, and that of our customers and partners, are as private as its owners want it to be.

To prepare for this new, privacy-centered era, enterprises should take steps *now* to safeguard the data they handle, following GDPR and CCPA regulations. Do this whether or not these laws apply to your country and organization. You should also ensure that the third parties you work with are doing the same. Taking advantage of technology privacy solutions or inventing your own should be a part of this effort.

Next, the savvy organization will publicize its commitment to data privacy, for example, publishing a "privacy bill of rights" as others have done.

Establishing yourself as a leader in the data privacy movement could help raise your company's profile head-and-shoulders above the competition.

We can bet on human ingenuity, but businesses need to play their part by prioritizing their customers' right to privacy and providing easy access services to do so.

Innovation can, and should, usher in a rebirth of privacy, giving individuals and companies unprecedented control over their data. Meanwhile, the digital age will continue to enrich our lives in countless ways.

This article reflects the opinions of the author.

Share article

Keywords:

DATA SECURITY PRIVACY

SUGGESTED ARTICLES

TRANSPARENCY

How can we solve the crisis in trust in business?

With cybercrime on the rise, and mistrust of how businesses handle data, it’s time to be more transparent and focus on security to win back the confidence of our customers.

privacy of thought header

FUTURE TECH

What does neural implant technology mean for digital privacy?

Thanks to brain-computer interfaces, telepathic communication could soon become a reality, but what does that mean for individual privacy?

body recognition eye

DATA AND PRIVACY

The good, the bad and the ugly of biometric authentication technology

Biometrics provide a quick and reliable way to identify and authenticate people by their unique physical characteristics. But does it help fight threats like cybercrime, and what does it mean for privacy?

AUTHOR INFO

Sherry Jones

Sherry Jones, an award-winning journalist and author, is CEO of CyberSmart Writing and Editing, specializing in cybersecurity, privacy and technology writing and executive ghostwriting.

MORE ARTICLES BY SHERRY JONES →

About Secure Futures

Secure Futures magazine is your go-to business guide for opinions, trends and insight into the world of technology and cybersecurity. We help your business to bring on the future. Brought to you by Kaspersky, the global cybersecurity experts.

Got an idea for a story you'd like us to cover? Contact the Editor.

What's coming next?

Be first to find out what's happening in tech, leadership and cybersecurity.

STAY AHEAD

Home Products

Kaspersky Anti-Virus

Kaspersky Internet Security

Kaspersky Total Security

Kaspersky Security Cloud

Kaspersky Security Cloud – Free

All Products

Small Business Products
1-50 EMPLOYEES

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

Medium Business Products
51-999 EMPLOYEES

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions
1000 EMPLOYEES

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Hybrid Cloud Security

All Solutions

Contact Us • About Us • Partners • Blog • Resource Center • Press Releases • Trust Kaspersky

Securelist • Threatpost • Eugene Personal Blog

Global