Opinion

Internet Privacy Is an Inalienable Right

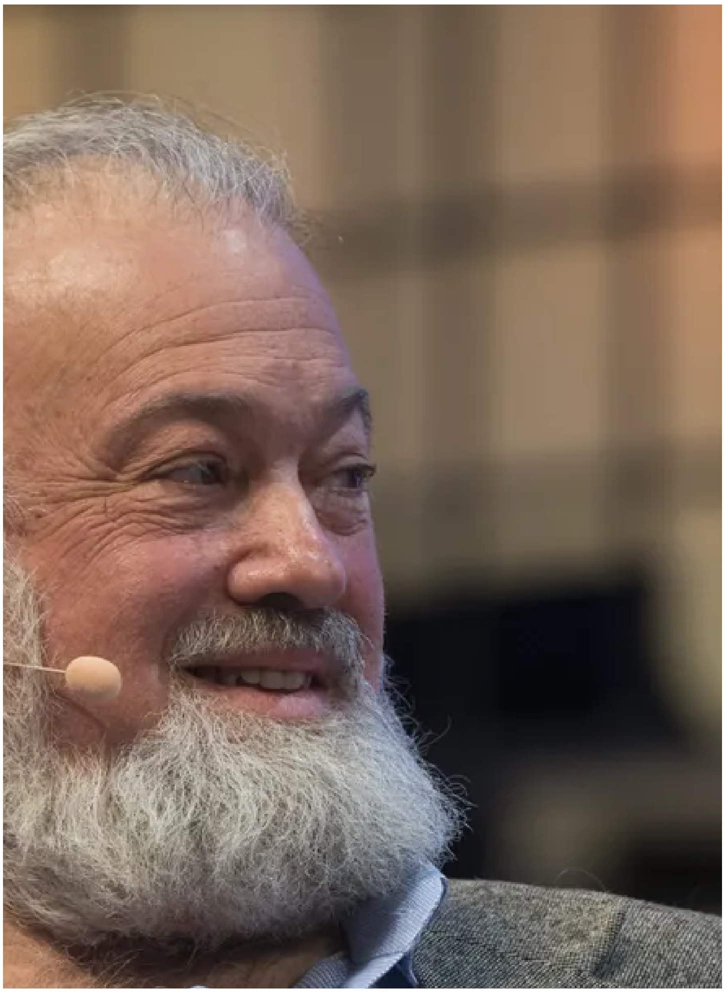
Digicash inventor David Chaum weighs in on the founding principles Web 3 needs. This post is part of CoinDesk's Privacy Week series.

By David Chaum

Jan 26, 2022 at 12:06 a.m.

Updated Sep 19, 2023 at 11:03 p.m.

Layer 2



Cryptographer David Chaum writes about the founding principles of Web 3. (Photo by Horacio Villalobos - Corbis/Getty Images)

As billions around the world continue to spend more and more of their lives online, making true digital privacy a reality has become imperative. At the same time, because of a series of scandals over the last two or three years, privacy has once again surfaced as a major – and very legitimate – public concern. The rapid emergence of Web 3 provides both a challenge and opportunity.

At first sight, the current reality is anything but encouraging. The entire business model of the “Big Tech” social media companies is built on collecting and selling users’ personal information to advertisers and political groups for the purpose of microtargeting. This information includes not only message content but all the metadata about what we search for or pay for, who we communicate with, when, how often and from where.

David Chaum, a pioneer in cryptography and in privacy-preserving and secure voting technologies, is the creator and founder of the xx network. In 1995, his company, DigiCash, created and deployed eCash, the first digital currency, which used Chaum's breakthrough blind-signature protocol. This post is part of CoinDesk's Privacy Week series.

'Father of Cryptocurrency' David Chaum Discusses …

In other words, Web 2 is essentially founded on the almost complete absence of user privacy and the exploitation of our personal information by huge centralized organizations. Almost as bad, these organizations maintain databases of this and other accumulated information about billions of us, which are breached by cybercriminals with shameful frequency.

To be sure, some social media companies promise or actually deliver end-to-end message encryption. But user metadata is much more valuable to these organizations than the message contents, as shown by the fact that Facebook, for instance, is proposing to offer "end-to-end" message content encryption while leaving user metadata in the clear so the company can continue to harvest and sell it. What's more, ever-more-powerful artificial intelligence (AI) is already being used to analyze the vast troves of scraped and sold data to both predict and manipulate user behavior. Such manipulation includes the tailoring and dissemination of disinformation for political ends. This dissemination is abetted by social-media algorithms that steer users toward more – and more extreme – sources of related disinformation with the ostensible goal of maintaining and increasing their "engagement."

Less apparent is that the deep structure of the internet from its origin was never intended to provide privacy. The U.S. Defense Advanced Research Projects Agency (DARPA), which commissioned the development of the TCP/IP message-packet protocol for the internet, explicitly prevented the encryption of packet headers, the digital "label" on each data packet forming part of a message that records source, destination, and transfer addresses.

Some encryption has since been added, but as we have learned from Edward Snowden among others, the National Security Agency (NSA) and other "intelligence" organizations, here and in other countries, easily and routinely gather metadata on internet traffic as part of what they call the "full take."

We can assume that advanced AI is also being used by these agencies to identify targets for message-content hacking even as (according to Snowden in 2014, backed by The Washington Post) 90% of those placed under surveillance in the U.S. are ordinary Americans, not the supposedly intended terrorist targets, as Snowden disclosed to The Washington Post in 2014.

Finally, when, not if, general-purpose quantum computers of sufficient power are developed, most of the types of encryption individuals currently rely on to preserve what weak, imperfect privacy and security they have will be worthless. That means all messages encrypted today will be readable retroactively.

Combined, this has a depressive effect on both democracy and individual freedom. It has long been established that widespread surveillance chills free speech and discourse. In countries with openly authoritarian governments, surveillance forestalls the emergence of democratic activity. In more democratic societies, the chilling effect extends to the expression of opinions that are outside the centrist “mainstream” of discourse.

This chilling effect extends to corporations. Anyone working for a company these days is well advised to avoid criticizing or complaining about their work environment using their work email, let alone proposing a worker organization like a protest group or a union.

See also:* *Bitcoin Dissidents: Those Who Need It Most

And even as more and more American states pass laws making it difficult to vote via mail or drop box – and even as the coronavirus pandemic drags on – the possibility of voting via the internet languishes.

What’s to be done?

Having watched this situation develop over four decades, I have come to believe the internet needs to be rebuilt from the ground up. The ground in this case is where the internet began: communications first between local university and laboratory networks and soon thereafter between private individuals. Just people exchanging information and ideas, talking about their lives, doing business and, crucially, discussing social and political issues.

Everyone has an inalienable right to associate privately, and ought to have a right to search for information anonymously. In other words, their personal information should belong to them, and they should be in complete control of it. Period.

This principle should be enshrined in law. There are very powerful vested interests hostile to the principle so it will take a large-scale social movement, online and off, to make informational sovereignty a legal right.

See also: ***'Father of Cryptocurrency' David Chaum Discusses Quantum Computing***

CoinDesk
Bitcoin $34160.65 0.87% Ethereum $1 Crypto Prices CoinDesk Market Index

The good news is that we can start building that foundation now, with existing cryptographic technologies, some of which are novel and others of which date back to the early days of the internet. Broadly, this new technological frontier is called Web 3 – a chance to reframe the web around users rather than corporations.

For Web 3 to achieve its aims, it needs to stand on a proper foundation. We require:

STORY CONTINUES BELOW

Recommended for you:

- How the Top 1% Covers Crypto
- First Mover Americas: Deutsche Bank Trials a SWIFT Alternative for Stablecoins
- The Hamas Funding Story Is Why Crypto Is Sick of the Mainstream Media

Decentralization: If personal communications are passed between teams of independently owned nodes, selected at random, second by second, from hundreds or thousands around the world working as a network collaborative, there is no centralized company for a government to pressure for user data or to insert spyware. Nodes can instead be organized on a blockchain to allow remuneration for participating in the network.

Elimination of metadata: Messages can be sent in such a way that metadata is destroyed at every node before forwarding to the next. This makes it virtually impossible to identify and link sender and receiver. Senders, however, can at will reveal the identity of receivers.

Quantum-resistant message encryption: As I mentioned, conventional encryption, based on techniques like the factorization of large numbers, is about to be rendered obsolete by quantum computers. Fortunately, quantum-resistant cryptography, whereby reverse-computing the encryption to obtain the message is mathematically infeasible, already exists.

These and related structures and techniques can be extended to existing essential functions of the internet like peer-to-peer payments, web browsing and shopping, and to new functions that we urgently need, like truly secure online voting. But everything starts with the basic principle that information about your life should belong to you.