The Sam Bankman-Fried Trial Full Coverage Here

Features

What If We Get Online Privacy Right? A Glimpse of 2035

Here's what a day in the life would look like if we nail privacy infrastructure, fix the policy and squash the forces behind that "creepy feeling." This post is part of CoinDesk's Privacy Week.

By Jeff Wilser Jan 25, 2022 at 9:40 p.m.

Updated Sep 19, 2023 at 11:03 p.m. Layer 2

(Rachel Sun/CoinDesk)

consensus 2024 by CoinDesk

10 Years of Decentralizing the Future

May 29-31, 2024 - Austin, Texas

The biggest and most established global hub for everything crypto, blockchain and Web3.

Register Now

Up

It's the year 2035. The bad news: There are no flying cars (although a cryogenically youthful Elon Musk is working on it), the United States is still bitterly divided, and the New YorkJets football team still doesn't have a quarterback.

But there is one silver lining: We've somehow fixed all the problems with online privacy.

It's done. We made it happen.

What would that world look like? How would your day-to-day life be different? That's the spirit of this exercise. It's not a prediction, it's not an argument, and it's not pretending to know exactly how we cracked the code. And of course all of this is very much in doubt.

"We're at a crossroads," said Tim Pastoor, a researcher in the Netherlands who focuses on digital identity. "We can either head towards a more utopian vision of how we do things, or a more dystopian vision."

This article is part of CoinDesk's Privacy Week series.

It's easy to imagine the dystopia. "Look at China, for example," Pastoor said. "If you say something the government doesn't like, you're not allowed onto planes and trains, and your kids aren't allowed to go to school, and you're not allowed to receive health care."

But what about the flip side? In one sense, perhaps the answer is dead simple: The world looks exactly how it does today in the United States, but your privacy is secure.

"If we succeed at fixing the infrastructure, then what we get is that the culture and the norms that we all currently share ... survive," said Zooko Wilcox, founder of the zcash privacy coin. So maybe just "Avoiding the China Scenario" is enough of a win.

But there are certain concrete, tangible ways that your life could improve. And some privacy experts think this is feasible.

"It's easy for people to think it's hopeless and there's nothing we can do," said Jon Callas, director of technology projects at the Electronic Frontier Foundation, a nonprofit devoted to defending digital privacy. "But there are things that are being done that have the potential to be very good. And if we do them right, we can have a better privacy-enhanced world."

Welcome to that vision of the future.

Privacy-protected social media and online shopping

7:30 a.m. *You log onto social media (which has deteriorated into an unholy blend of one-second videos and emojis), eager to comment on the presidential contest between Chelsea Clinton and Barron Trump. Logging in is a breeze. You don't need to remember any passwords. Instead, you use a "Privacy Broker" – a company that acts as your intermediary and shields your data.*

Apple is already working on early versions of this solution, such as its "Private Relay" now in beta. "We want more people to be doing this," Callas said.

9:37 a.m. *You go online to buy a few of the basics: Toenail fungus remover, cold sore treatment, a BDSM kit, medicine for diarrhea and a vintage album from One Direction.*

You're not embarrassed. You know you won't be served up ads for toe fungus for the next month. And you know that the data cannot be turned over to the government ... or anyone.

That's not the case today.

"Under the Bank Secrecy Act (BSA), all sorts of transactions from banks and other financial intermediaries [can be] turned over to the government, by default, without a warrant," said Marta Belcher, general counsel at Protocol Labs, a research and development center for network protocols. Thanks to a court precedent called the "third-party doctrine," in today's world, "If any third party has your data, you lose your reasonable expectation of privacy."

So the BSA would need to be changed to protect digital privacy. Belcher is optimistic that will happen by 2035, saying, "I think that the warrantless financial surveillance under the BSA is unconstitutional, and if it went up to the Supreme Court, I believe they would agree."

In-person shopping in a privacy-protected world

12:04 p.m. *On your lunch break you head to the grocery store, and even offline shopping is now a snap.*

The grocery store won't collect your data. The police won't get your data.

"I would like to walk into a grocery store and pick up all my groceries, and walk out, and know that I'm paying a fair price," Wilcox said. "And I'm safe doing this, because I'm not giving anyone ... the right to watch me all the time."

In the scenario Wilcox imagines, "The computer that I carry around with me is negotiating with the grocery store computer and making sure that both people are happy with the deal ... so I don't have to think about it."

Privacy-preserving IDs

12:37 p.m. *While you're out running errands, you stop by the liquor store to buy a bottle of wine. The cashier asks to see your ID. He's a sketchy-looking dude. He stares at you while you shop, he's openly leering and you don't love the idea of showing him an ID that reveals your full name, much less your home address.*

But you don't need to.

You flash him an ID, he scans a barcode, and the only thing he can see is the only thing he needs to see: that you are at least 21. Done and done. Creepy Dude can't see your address or age.

This is thanks to the magic of zero-knowledge proofs – basically an encrypted way of showing that a statement is "true" without revealing the underlying information used to reach that conclusion. They could be especially useful for IDs. "Privacy preserving IDs are happening," said callas, who has written extensively on the subject.

"Colorado is at the forefront" of innovating with mobile and privacy-respecting drivers licenses, Callas said, along with "half a dozen other states."

Consumer control of targeted ads

3:00 p.m. *You see a hyper-specific ad: The exact shirt you were hoping would go on sale, and now it's 50% off.*

You weren't served up the ad because some algorithm was stalking your online behavior; instead, you were empowered to get what you want.

Pastoor has a theory for how this could work. “It’s more of a white-listing principle,” he said. Instead of centralized companies cranking out algorithms from your trove of personal data, you would simply provide information – the “white list” – of things that interest you.

“You add a shirt to the wish list, and you opt into service providers that serve you the best possible deal,” Pastoor said. “If they start spamming you, then you can remove them from your network.” The idea shares DNA with the technologist Doc Searls’ vision of an “intention economy,” where individuals and buyers control the data and set the terms ... not the centralized sellers.

4:17 p.m. *You see another online ad, also hyper-specific, for the exact sofa you just searched for... and you are not creeped out.*

You have no reason to be. In this 2035 world that respects privacy, thanks to a combination of things that we get right – such as the above “white list” idea, or privacy regulation, or more decentralized solutions, or competitive privacy brokers – you know that your data is not being used to track or target you, and you can relax.

Contrast this to today. Amie Stepanovich, vice president of U.S. policy at the Future of Privacy Forum, said that if we get online privacy right, then even if our day-to-day lives won’t look all that different, but they will feel different.

The future could lack the “creepy element” of how we now view technology, she said. We put up with this creepy feeling (like the kind we get from hyper-targeted ads) simply because we have no choice; it’s the only way to join online society. For many, it’s an agonizing tradeoff.

We often feel an eerie sense of invasion – that Big Tech’s omniscient knowledge of our personal data is used to target and define us. “In a world where those types of invasive activities aren’t allowed to happen, people should be more comfortable with technology, because they know their rights won’t be abused,” Stepanovich said.

The right to be forgotten

5:08 p.m. *You have a hot take about Tom Brady's game last night. Brady threw four interceptions and fumbled twice, and you go online to joke that this is the year that the 57-year-old hangs up his cleats.*

Maybe your take won't age well. (You've posted the same thing for 16 years; you're always wrong.) But it doesn't matter, because soon the post will auto-delete.

"My hot take on last night's [Stephen] Colbert episode really only needs to be around for a week," said Callas, who personally uses a tool called Semiphemeral that scrubs and deletes his online posts, subject to certain parameters. (Tweets with X number of retweets might remain, for example.)

Callas imagines this kind of service expanding and going mainstream in the future, as it tackles a different flavor of online privacy – we forget that we're leaving a public digital trail of all of our fleeting opinions, no matter how spontaneous or dumb.

"People should be able to shed their past," Callas said. "If people can't shed their past, they can't ever change their mind."

Employee privacy

7:00 p.m. *You chill out to watch "Fast and the Furious 23." And while you watch Vin Diesel race cars around the rings of Saturn, something magical happens: Nothing.*

More specifically, there are no emails, texts or Slacks from your boss. Your workplace respects your privacy.

"No texts or emails after 5 p.m.," said U.S. military whistle-blower and privacy activist Chelsea Manning, who views the breaching of our personal time as an overlooked violation of privacy.

She notes that long ago, in a simpler time, we worked a 40-hour week where we punched out at 5 p.m., commuted home and then enjoyed our evening.

"We don't have that anymore," she said. "And that is a privacy issue. That's your employer invading your privacy. I believe this."

Sexual privacy

10:30 p.m. *You head to an adult website. (Yes. That kind of website. We're all human.) Rather than just watching the free clips, you decide to splurge on some premium content. And thanks to a combination of cryptocurrency adoption and new legal safeguards, no one is able to exert financial censorship.*

"This is something ordinary people don't notice, but there's a subset of people for whom it's already a huge problem," said Belcher, who notes that OnlyFans, for example, was forced to ban sexual content to appease Visa and Mastercard.

CoinDesk
Bitcoin $34,150.88 -0.37% Ethereum $1, Crypto Prices CoinDesk Market Index

people can transact openly, without Visa and Mastercard dictating what speech is and is not allowed on the internet."

Peace of Mind

12:00 a.m. *You go to bed not worrying that anything you have done today will be used against you, sold to third parties or somehow embarrass you.*

You relax.