Simple fixes to preserve privacy in an AI-enabled world of smart fridges and fitbits

April 22 2022, by Toby Walsh

Credit: Skylar Kang from Pexels

The Second Law of Thermodynamics states that the total entropy of a system—the amount of disorder—only ever increases. In other words, the amount of order only ever decreases.

Privacy is similar to entropy. Privacy is only ever decreasing. Privacy is not something you can take back. I cannot take back from you the knowledge that I sing Abba songs badly in the shower. Just as you can't take back from me the fact that I found out about how you vote.

There are different forms of privacy. There's our digital online privacy, all the information about our lives in cyberspace. You might think our digital privacy is already lost. We have given too much of it to companies like Meta and Google. Then there's our analog offline privacy, all the information about our lives in the physical world. Is there hope that we'll keep hold of our analog privacy?

Toasters, locks and watches

The problem is that we are connecting ourselves, our homes and our workplaces to lots of internet-enabled devices: smartwatches, smart lightbulbs, toasters, fridges, weighing scales, running machines, doorbells and front door locks. And all these devices are interconnected, carefully recording everything we do.

Our location. Our heartbeat. Our blood pressure. Our weight. The smile or frown on our face. Our food intake. Our visits to the toilet. Our workouts.

These devices will monitor us 24/7, and companies like Google and Amazon will collate all this information. Why do you think Google bought both Nest and Fitbit recently? And why do you think Amazon acquired two smart home companies, Ring and Blink Home, and built their own smartwatch? They're in an arms race to know us better.

The benefits to the companies our obvious. The more they know about us, the more they can target us with adverts and products. There's one of Amazon's famous "flywheels" in this. Many of the products they will sell

us will collect more data on us. And that data will help target us to make more purchases.

The benefits to us are also obvious. All this health data can help make us live healthier. And our longer lives will be easier, as lights switch on when we enter a room, and thermostats move automatically to our preferred temperature. The better these companies know us, the better their recommendations will be. They'll recommend only movies we want to watch, songs we want to listen to and products we want to buy.

But there are also many potential pitfalls. What if your health insurance premiums increase every time you miss a gym class? Or your fridge orders too much comfort food? Or your employer sacks you because your smartwatch reveals you took too many toilet breaks?

With our digital selves, we can pretend to be someone that we are not. We can lie about our preferences. We can connect anonymously with VPNs and fake email accounts. But it is much harder to lie about your analog self. We have little control over how fast our heart beats or how widely the pupils of our eyes dilate.

We've already seen political parties manipulate how we vote based on our digital footprint. What more could they do if they really understood how we responded physically to their messages? Imagine a political party that could access everyone's heartbeat and blood pressure. Even George Orwell didn't go that far.

Worse still, we are giving this analog data to private companies that are not very good at sharing their profits with us. When you send your saliva off to 23AndMe for genetic testing, you are giving them access to the core of who you are, your DNA. If 23AndMe happens to use your DNA to develop a cure for a rare genetic disease that you possess, you will probably have to pay for that cure.

The 23AndMe terms and conditions make this very clear:

"You understand that by providing any sample, having your Genetic Information processed, accessing your Genetic Information, or providing Self-Reported Information, you acquire no rights in any research or commercial products that may be developed by 23andMe or its collaborating partners. You specifically understand that you will not receive compensation for any research or commercial products that include or result from your Genetic Information or Self-Reported Information."

A private future

How, then, might we put safeguards in place to preserve our privacy in an AI-enabled world? I have a couple of simple fixes. Some are regulatory and could be implemented today. Others are technological and are something for the future, when we have AI that is smarter and more capable of defending our privacy.

The technology companies all have long terms of service and privacy policies. If you have lots of spare time, you can read them. Researchers at Carnegie Mellon University calculated that the average internet user would have to spend 76 work days each year just to read all the things that they have agreed to online. But what then? If you don't like what you read, what choices do you have?

All you can do today, it seems, is log off and not use their service. You can't demand greater privacy than the technology companies are willing to provide. If you don't like Gmail reading your emails, you can't use Gmail. Worse than that, you'd better not email anyone with a Gmail account, as Google will read any emails that go through the Gmail system.

So here's a simple alternative. Under my plan, all digital services must provide four changeable levels of privacy.

Level 1: They keep no information about you beyond your username, email and password.

Level 2: They keep information on you to provide you with a better service, but they do not share this information with anyone.

Level 3: They keep information on you that they may share with sister companies.

Level 4: They consider the information that they collect on you as public.

You can change the level of privacy with one click from the settings page. And any changes are retrospective, so if you select Level 1 privacy, the company must delete all information they currently have on you, beyond your username, email and password. In addition, there's a requirement that all data beyond Level 1 privacy is deleted after three years unless you opt in explicitly for it to be kept. Think of this as a digital right to be forgotten.

I grew up in the 1970s and 1980s. My many youthful transgressions have, thankfully, been lost in the mists of time. They will not haunt me when I apply for a new job or run for political office. I fear, however, for young people today, whose every post on social media is archived and waiting to be printed off by some prospective employer or political opponent. This is one reason why we need a digital right to be forgotten.

More friction may help. Ironically, the internet was invented to remove frictions—in particular, to make it easier to share data and communicate more quickly and effortlessly. I'm starting to think, however, that this

lack of friction is the cause of many problems. Our physical highways have speed and other restrictions. Perhaps the internet highway needs a few more limitations too?

One such problem is described in a famous cartoon: "On the internet, no one knows you're a dog." If we introduced instead a friction by insisting on identity checks, then certain issues around anonymity and trust might go away. Similarly, resharing restrictions on social media might help prevent the distribution of fake news. And profanity filters might help prevent posting content that inflames.

On the other side, other parts of the internet might benefit from fewer frictions. Why is it that Facebook can get away with behaving badly with our data? One of the problems here is there's no real alternative. If you've had enough of Facebook's bad behavior and log off—as I did some years back—then it is you who will suffer most.

You can't take all your data, your social network, your posts, your photos to some rival social media service. There is no real competition. Facebook is a walled garden, holding onto your data and setting the rules. We need to open that data up and thereby permit true competition.

For far too long the tech industry has been given too many freedoms. Monopolies are starting to form. Bad behaviors are becoming the norm. Many internet businesses are poorly aligned with the public good.

Any new digital regulation is probably best implemented at the level of nation-states or close-knit trading blocks. In the current climate of nationalism, bodies such as the United Nations and the World Trade Organization are unlikely to reach useful consensus. The common values shared by members of such large transnational bodies are too weak to offer much protection to the consumer.

The European Union has led the way in regulating the tech sector. The General Data Protection Regulation, and the upcoming Digital Service Act and Digital Market Act are good examples of Europe's leadership in this space.

National laws set precedents

A few nation-states have also started to pick up their game. The United Kingdom introduced a Google tax in 2015 to try to make tech companies pay a fair share of tax. And shortly after the terrible shootings in Christchurch, New Zealand, in 2019, the Australian government introduced legislation to fine companies up to 10% of their annual revenue if they fail to take down abhorrent violent material quickly enough. Unsurprisingly, fining tech companies a significant fraction of their global annual revenue appears to get their attention.

It is easy to dismiss laws in Australia as somewhat irrelevant to multinational companies like Google. If they're too irritating, they can just pull out of the Australian market. Google's accountants will hardly notice the blip in their worldwide revenue. But national laws often set precedents that get applied elsewhere. Australia followed up with its own Google tax just six months after the UK.

California introduced its own version of the GDPR, the California Consumer Privacy Act, just a month after the regulation came into effect in Europe. Such knock-on effects are probably the real reason that Google has argued so vocally against Australia's new Media Bargaining Code. They greatly fear the precedent it will set.

That leaves me with a technological fix. At some point in the future, all our devices will contain AI agents helping to connect us that can also protect our privacy. AI will move from the center to the edge, away from the cloud and onto our devices. These AI agents will monitor the

data entering and leaving our devices. They will do their best to ensure that data about us that we don't want shared isn't.

We are perhaps at the technological low point today. To do anything interesting, we need to send data up into the cloud, to tap into the vast computational resources that can be found there. Siri, for instance, doesn't run on your iPhone but on Apple's vast servers. And once your data leaves your possession, you might as well consider it public. But we can look forward to a future where AI is small enough and smart enough to run on your device itself, and your data never has to be sent anywhere.

This is the sort of AI-enabled future where technology and regulation will not simply help preserve our privacy, but even enhance it.

Provided by The Conversation

Citation: Simple fixes to preserve privacy in an AI-enabled world of smart fridges and fitbits (2022, April 22) retrieved 10 April 2024 from https://techxplore.com/news/2022-04-simple-privacy-ai-enabled-world-smart.html