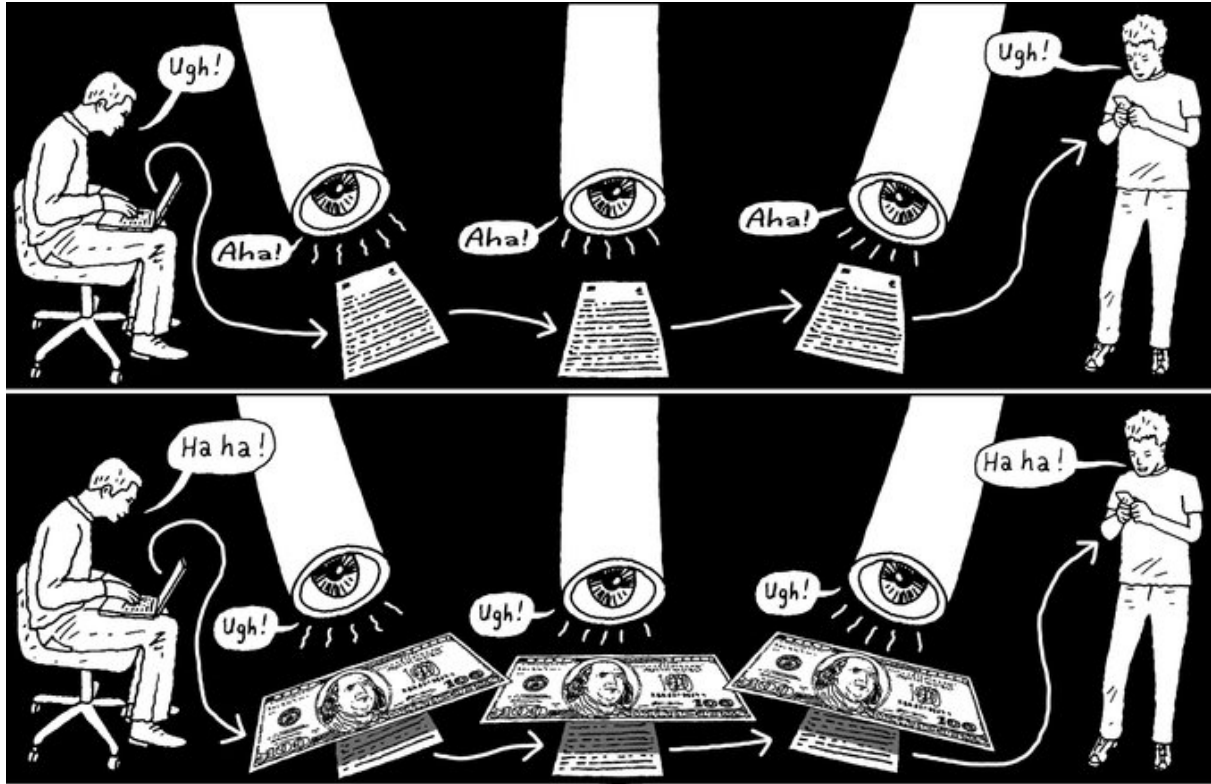


# Has Privacy Become a Luxury Good?

By JULIA ANGWIN MARCH 3, 2014

Photo



Credit Peter Arkle

LAST year, I spent more than \$2,200 and countless hours trying to protect my privacy.

Some of the items I bought — a \$230 service that encrypted my data in the Internet cloud; a \$35 privacy filter to shield my laptop screen from coffee-shop voyeurs; and a \$420 subscription to a portable Internet service to bypass untrusted connections — protect me from criminals and hackers. Other products, like a \$5-a-month service that provides me with disposable email addresses and phone numbers, protect me against the legal (but, to me, unfair) mining and sale of my personal data.

In our data-saturated economy, privacy is becoming a luxury good. After all, as the saying goes, if you aren't paying for the product, you *are* the product. And currently, we aren't paying for very much of our technology.

Not long ago, we would have bought services as important to us as mail and news. Now, however, we get all those services for free — and we pay with our personal data, which is spliced and diced and bought and sold.

Consider Google, which scans what you write in Gmail to offer advertisers a chance to promote their items based on your missives. Or a visit to an online news site where your data is secretly auctioned and sold before the page loads. Or Facebook, which allows marketers to turn your status updates into ads for their products.

<http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html>

Those who aren't bothered by that exchange should keep in mind that our data is used not just for advertisements. It has also been used to charge people different prices based on their personal information. It has been used to provide different search results to different people based on their political interests. It has been used by the government to identify possible criminal and terrorist suspects. Just last week, we learned that the British government had intercepted and archived still images from millions of Yahoo webcam chats around the world, whether or not the participants were suspected of wrongdoing.

The more we learn about how our data is being harnessed — and how it may be exploited in the future — the more likely we are to re-evaluate the true cost of these supposedly free services. And some of us will start trying to buy our way out of the trade-your-data-for-services economy.

But, as I have learned, it isn't cheap or convenient to start buying privacy. I spend annoying amounts of time updating software or trying to resolve technical difficulties when my different privacy-protecting services conflict with one another.

It all reminds me of the early days of the organic food movement, when buying organic often meant trekking to inconveniently located, odd-smelling stores and paying high rates for misshapen apples. Only the devoted few were willing to suffer the hassles.

Over time, however, the number of people worried about chemicals in their food grew large enough to support a robust market. The stores eventually became better looking, the apples were less misshapen, and organic food entered the mainstream of American life.

A similar evolution in the personal-data-protection market is underway. Traffic to the privacy-protecting search engine DuckDuckGo has more than doubled since Edward J. Snowden revealed vast government surveillance programs last June. The Blackphone, a \$629 not-yet-released Android-based smartphone that will have privacy-protecting software installed to allow users to send encrypted texts and make encrypted calls, is being pre-ordered by the thousands. And last year, a New York entrepreneur, Adam Harvey, sold out of his first run of the OFF Pocket — an \$85 cellphone case that blocks signals to and from the phone. “My vision is that privacy won't be given to you as a law completely,” he told me. “You have to commercialize it so people can speak with their money.”

Standing in the way of the widespread adoption of these tools, however, is the problem of verification. I have Mr. Harvey's OFF Pocket and it seems to block the cell signals, but I don't know for sure that it works as promised. The same is true with the Blackphone, or DuckDuckGo's privacy policies. I hope their claims are true, but there are few trusted third parties to verify them.

This was brought home to me when I signed up for a service from TrustedID. For \$35, the company promised to opt me out of some of the biggest American data brokers. A few months later, I contacted those brokers to confirm that my information had been removed from their databases. It turned out that TrustedID had failed to process more than half of the opt-outs. The service has since been suspended.

As more privacy-protecting services pop up, we need to consider two important questions: Can we ensure that those who can afford to buy privacy services are not being deceived? And even more important, do we want privacy to be something that only those with disposable money and time can afford?

The food industry can offer some possible answers to those questions. Our government enforces baseline standards for the safety of all food and has strict production and labeling requirements for organic food. It may be time to start doing the same for our data.

[Julia Angwin](#) is a senior reporter at ProPublica and the author of “Dagnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance.”