Privacy for Sale

On 16 September 2021, I was perusing my morning newspaper (well, actually, my morning news website) and was struck by this headline: "The Battle for Digital Privacy Is Reshaping the Internet."[1] Of course, I immediately read the article, which, in summary, said that major technology firms are in the process of rethinking their stances on data privacy. Some, led by Apple, are choosing to give their customers the ability to prevent their web browsing activity from being tracked for sale to advertisers. Others, notably Facebook, are pushing back, saying that the ability to discern buyers' online preferences is critical to the success of small retailers. Google is also involved, with its position somewhere in the middle: "Give me privacy, but not yet."

The outcome, so the article proposes, will be that many web-based applications that we do not pay for today "…will make people pay for what they get online by levying subscription fees and other charges instead of using their personal data."[2] The ramifications of charging for privacy in the use of widely used applications are, to my mind, significant and worth exploring.

STEVEN J. ROSS | CISA, CDPSE, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal's* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

The Price of Privacy

We have long given up some of our private information to have a bank account, medical care and cable television. At the same time, we have relied (sometimes mistakenly) on the companies that provided these products and services not to share our data without our permission. We had no such implicit deal when we started using applications to search the Internet, guide us in our travels and communicate with one another. These services are paid for in the coin of personal data. If we had to pay actual money for Internet services in return for protecting our privacy, would we do it?

Some people would, no doubt. They feel victimized by what author Shoshana Zuboff calls "surveillance capitalism."[3] They believe, with some justification, that their every move is being tracked and used to manipulate them. It is worrisome enough that they would pay to stop it. But what of those who do not care if they are bombarded with advertisements? And what of those who cannot afford to pay?

This might result in a two-tier Internet, one with privacy for the well-to-do and an exploitative one for everyone else. Individuals would have to determine whether it was worth paying for each search, each map, each headline, each email.[4] It would be a delicate decision for those who are privacy conscious. One person might pay .001 US cents per search, but not a dollar. Another might find a dollar a fair price and someone else would not find any charge to be worth paying.

It is more likely that applications would be priced on a subscription basis. I am sure that I am like many people in that I use search and mapping applications frequently, so I might pay a reasonable fee for them. Who is to say what is reasonable? Would the market advantage accrue to the better, higher-priced search tool? Or would it go to the less costly application, funded by advertisers who skew the results in their own favor?

Societal Implications

In the 1970s, there was an expression in the United States: What if they gave a war and nobody came? In

the near future, we well might ask what if they sold privacy and nobody bought it?

There has been a spate of laws passed in recent years to guarantee data privacy or at least to make violations of privacy costly to the offenders. Passage of these laws was based, at least in theory, on the will of the people in each jurisdiction. If placing a price on privacy resulted in a large share of the populace, perhaps a majority, choosing to forego it, what does that say about society's commitment to keeping personal information confidential?

Might the entry of privacy into the marketplace perversely undermine support for it? It is not clear that this would happen, but the possibility should give pause to privacy advocates. The next law restricting the use of personal information might become considerably harder to get through the legislature if there were evidence that people did not care.

Delivering Privacy

Is privacy a commodity? Or is there a range of privacy that might be for sale? Perhaps the market will support different levels of privacy, just as it supports different levels with premium pricing for airplane seats, credit cards and Scotch whiskey. Perhaps bronze-level privacy would allow an application vendor to sell a person's data to a commercial enterprise but not the government. Only platinum privacy would prohibit release of personal information to anyone at all. Is that the way we want data to be handled? Is that the sort of society we want to have?

Privacy cannot be delivered by the pound, the box, or the bottle, so if someone were to buy privacy, how would that person know he or she had received it? For example, consider someone who had paid for privacy in search and mapping applications but not in images. If that individual were planning a vacation in the south of France and checked up on instructions on the Route de Soleil and looked at pictures of the Côte d'Azur, he or she might be deluged with ads for restaurants in Cannes and Nice. Was that a failure of privacy in the mapping application or the absence of it in the images app? How could the buyer ever know?

If the buyer cannot even beware, how can the implicit contract (or, perhaps, an explicit contract) entered into with the application vendor be enforced. Today, any use of hundreds of applications results in an ephemeral trail of personal metadata that can be monetized by the vendor for sale to those who want to know what users want to buy, where they are and where they are going. In a possible future in which privacy can be sold, these vendors would need to recognize who is trying to access what and with which application. Before returning the requested information, the vendor would need to determine whether that person's subscription is paid. If so, the requester's metadata would not be retained. Or if they were retained, that metadata would not be sold. The possibility—no, the likelihood—of privacy miscues is very high.

Decisions to Make

Hardly a day passes in which I do not use applications for searching the Internet, getting the latest news, finding my way, listening to music and checking the weather. Nor does a day pass in which I am not inundated with advertisements related to things for which I may have looked. Perhaps I have a high degree of sales resistance, but I have never bought anything that I saw in one of those ads, nor even clicked on one. Do I really mind if I am being surveilled in this way? Would I pay to not receive the commercial messages? And if so, how much?

These are decisions I may soon have to make. As much as I value privacy—both my own and everyone else's so that society can be livable—I am not sure what I will do.

Endnotes

1 Chen, B. X.; "The Battle for Digital Privacy Is Reshaping the Internet," *The New York Times*, 16 September 2021, *https://www.nytimes.com/2021/09/16/technology/digital-privacy.html?searchResultPosition=3*

2 *Ibid*.

3 Zuboff, S.; *The Age of Surveillance Capitalism*, Hachette Book Group, USA, 2019

4 As I write this paragraph, I am looking at my smartphone and I cannot honestly say how much I would pay for any of the apps I see there. And I am a certified privacy engineer!

LOOKING FOR MORE?

- Read *Privacy by Design and Default: A Primer. www.isaca.org/Privacy-by-Design*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*