Un-Privacy by Design

At the end of my last column,[1] I allowed myself a bit of a sneer at the notion of "privacy by design." This concept was first publicly enunciated by Ann Cavoukian, then the Information and Privacy Commissioner for the Canadian province of Ontario.[2] I am all for data privacy and for well-designed systems. I just do not see, as a practical matter, how to design it.

I do have the necessary guidance, enshrined in Article 25 of the European Union's General Data Protection Regulations (GDPR) in three not particularly pithy sentences, the first of which is definitional:

> *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*[3]

I challenge anyone to remember the beginning of this 114-word sentence by the end of it. It was clearly written by a committee. Let me help: I believe it says that people should think about the technology, context, cost and risks and then do their best to use available tools to design privacy into systems. But is there a need to design privacy? After all, no one designs un-privacy.

We-e-e-e-l, that is not quite true.

Cyberthefts of Personal Information

Cyberattackers do not include privacy in their designs. Quite the reverse, in fact. All the recent great thefts of personal information are by definition privacy breaches, including data stolen from Equifax[4] in the United States, British Airways,[5] Caisse Desjardins in Canada,[6] Uniqlo in Japan[7] and from virtually the entire population of Bulgaria.[8] Unquestionably, the victimized organizations had some technological or procedural shortcoming that criminals exploited. But was that a failure of design? With absolutely no inside information on my part, I am willing to wager that none of their system architects said, "Oh, what the heck, let them steal whatever they like."

There would be global chaos if every organization that suffers a cybertheft of personal information were then to be subjected to the wrath of privacy regulators. Happily, I see no evidence that this has been the case, although some of the security inadequacies that have come to light were certainly egregious. Information security professionals who would design privacy into their systems should do everything they can to deter cyberattacks, which I think they are already doing.

"Big Tech"

There are those giant technology companies whose business model consists of obtaining personal information in exchange for "free" services and selling it onward. Contrary to the popular wisdom, there is such a thing as a free lunch, but there is no zero-cost lunch; somebody pays. And if you are using one of these "free" browser, video or map applications, and many more, then you are paying in

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2nbvubZ

Steven J. Ross, CISA, AFBCI, CISSP, 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 coin of your personal information.[9] It would seem that this must be an example of un-privacy by design, but is it really?

The essence of a privacy violation is the use of personal information for purposes other than those for which it was collected. This is the central contention in the EU's €50 million fine against Google.[10] But a reading of Google's privacy policy on its website may tell a different story. Now, most people have not read Google's privacy statement,[11] but in the interests of deep research, I took an afternoon out of my life and read the 27-page document.

What I found is that Google tells everyone exactly what it will do with their personal information if they use a Google service. They say they will collect as much personal information as they can.[12] And they will share it with other organizations that want to sell stuff.

> *For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for 'pizza.'*[13]

They explain it in simple, clear English (and I assume other languages, though I did not check). Users may or may not like these practices, but they are not privacy violations because everyone has been told what Google is doing. Information security professionals who would design privacy into their systems should read the fine print and, in some cases, they should write it.

The System Design Process

There are also all the cases in which people's privacy is violated not because someone designed the systems to disclose personal information, but because those systems were not designed to protect that information. It is not that the designers wanted to do something bad; they just could not spare the time to do the right things. Sins of omission can be as problematic as those of commission.

A designer conceptualizes a system to serve a particular purpose, writes it, tests it to make sure it works at all and then releases it for use. Having made sure (well, fairly sure) that the system does what it is supposed to do, making sure that it does not do what it is not supposed to do—such as disclosing people's data—just stands in the way of getting the system into production.[14]

> "THE BEST PRIVACY CONTROLS CAN BE OVERRIDDEN BY POORLY TRAINED USERS."

By "system," I mean more than just computer programs. I include the infrastructure in which those programs execute, the procedures with which they are used, the people who use them and the training those people receive. The best privacy controls can be overridden by poorly trained users. I was recently affected myself when someone in my doctor's office sent an email cc'd to all patients taking a particular medicine. The medicine in question was not controversial, but my health records should never have been publicized.[15]

So, if privacy is not a part of a system's design, then it ought to be a part of its quality assurance, risk evaluation, audit…and security. There really ought to be privacy professionals on the case as well, whether as a part of the information security

function or distinct from it. In many cases, those in charge of privacy are concerned with legality and compliance and are not well versed in the details of information technology. So information security professionals who want to see privacy designed into their systems need to step up and be a part of the design process, as well as testing and validation once a system is designed.

Endnotes

1 Ross, S. J.; "Why Do We Need Data Privacy Laws?" *ISACA® Journal*, vol. 5, 2019, *https://www.isaca.org/archives.* Specifically, I wrote "Designing 'privacy' into systems wherein a breach will have no real consequences diminishes the attention that is required to protect us against truly intrusive systems."

2 Cavoukian, A.; "Privacy by Design: The Seven Foundational Principles," IAPP Resource Center, *https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/*

3 Intersoft Consulting, "Art. 25(1) GDPR: Data Protection by Design and by Default," European Union, 2016, *https://gdpr-info.eu/art-25-gdpr/*

4 Siegel Bernard, T.; T. Hsu; N. Perlroth; R. Lieber; "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *The New York Times*, 7 September 2017, *https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?searchResultPosition=8*

5 Porter, J.; "British Airways Faces Record-Breaking GDPR Fine After Data Breach," *The Verge*, 8 July 2019, *https://www.theverge.com/2019/7/8/20685830/british-airways-data-breach-fine-information-commissioners-office-gdpr*

6 Monpetit, J.; "Personal Data of 2.7 Million People Leaked From Desjardins," *CBC News,* 20 June 2019, *https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297*

7 Huang, E.; "Hackers Access Data From More Than 460,000 Accounts at Uniqlo's Online Store," *CNBC*, 14 May 2019, *https://www.cnbc.com/2019/05/14/japans-uniqlo-says-hackers-access-data-from-460000-online-accounts.html*

8 Krasimirov, A.; T. Tsolova; "In Systemic Breach, Hackers Steal Millions of Bulgarians' Financial Data," *Reuters,* 16 July 2019, *https://www.reuters.com/article/us-bulgaria-cybersecurity/bulgarian-tax-agency-says-hackers-stole-millions-of-financial-records-idUSKCN1UB0MA*

9 *Op cit* Ross

10 Satraiano, A.; "Google Is Fined $57 Million Under Europe's Data Privacy Law," *The New York Times*, 21 January 2019, *https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html*. Neither I nor ISACA® wish to express any opinions on the substance of the law case. But inasmuch as the penalty assessed against Google is among the most prominent in the world, it seems only fair to make Google the subject of a discussion on companies that aggregate and sell personal information.

11 As of the time of writing. The date is important, because it is 22 January 2019, one day *after* the EU privacy judgement. I have not read the privacy statement in effect before that date. Google, Privacy Policy, *https://policies.google.com/privacy*

12 *Ibid*. Except "…sensitive categories, such as race, religion, sexual orientation, or health…"

13 *Ibid*.

14 Ross, S. J.; R. G. Parker; "The Brave Old New World of Privacy," *ISSA Journal*, September 2018, p. 21

15 This is reminiscent of a much more significant case in 2001 involving a manufacturer of Prozac. Yamey, G.; "Eli Lilly Violates Patients' Privacy," *The BMJ*, 14 July 2001, *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1120743/*

Enjoying this article?

- Read *Implementing the General Data Protection Regulation. www.isaca.org/Implementing-GDPR*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*