Why Do We Need Data Privacy Laws?

There has been no shortage of data privacy laws enacted in the past few years. The one that has received the most attention is the EU General Data Protection Regulation (GDPR), in force since 25 May 2018. In the United States, California and Maine have passed new laws with the promise of more to come. Brazil's General Data Protection Law goes into effect in 2020. Many countries, including Bosnia and Herzegovina, Monaco, Montenegro, North Macedonia, and Ukraine, have amended their existing data protection legislation to align with GDPR.[1]

Why Do We Need Laws?

Generally, laws exist to correct behaviors that various jurisdictions consider to be unacceptable, everything from homicide to littering. (I leave it to the reader to determine where violations of data privacy fall along that spectrum.) It is not as though there were a sudden realization that personally identifiable information (PII) was at risk of disclosure; there were plenty of data privacy laws already on the books. GDPR itself replaced the EU Data Protection Directive of 1995.[2] The Canadian Personal Information Protection and Electronic Documents Act (Pipeda) was enacted in 2000.[3] Japan's Act on the Protection of Personal Information (APPI) dates back to 2003.[4] In fact, almost all countries have had some form of privacy legislation in effect in this century or before. So what has caused so many governments around the world[5] to upgrade their privacy laws recently?

I have to admit to a degree of skepticism about these new, more assertive data privacy laws. I am a member in good standing of the Privacy Supporters Club. (I have in my files some correspondence with my US congressman supporting the US Privacy Act of 1974.) It is just that when I read that some new law will finally make PII truly private, I feel as though I have heard this song before.

Fines and Enforcement

If people and organizations were not observing the EU Data Protection Directive, what would lead us to believe that GDPR will make things any different? Ah yes, there are harsh financial penalties for disregarding GDPR. And, indeed there were 59,000 reported GDPR breaches in the first eight months the law was in effect. That sure is a lot. But there were only 91 financial penalties issued, for a total of €56 million, of which the vast preponderance was the €50 million fine issued to Google.[6, 7]

I am certain that Google is not fond of paying out so much money for not properly disclosing to users how data are collected across its services—including its search engine, Google Maps and YouTube—to present personalized advertisements.[8] However, Google's parent company, Alphabet, reported US$142

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/2Ys8QJg

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.

Enjoying this article?

- Read *Maintaining Data Protection and Privacy Beyond GDPR Implementation. www.isaca.org/Data-Protection-Beyond-GDPR*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/online-forums*

billion in revenues for 2018. Is the fine that was levied on the company enough to significantly change the way Google does business[9] or make a serious difference to data privacy in Europe?

Castles in Spain

I suggest that the spate of new data privacy laws has come about because governments are aware of their inability to constrain the use of PII for purposes other than those for which it was collected, the very core of data privacy. They cannot constrain the enterprises that have arisen as a threat to that definition. This century has seen the arrival and massive growth of organizations whose entire business model is the collection of personal information for the purpose of selling it to advertisers and others trying to reach targeted market segments. With very limited exceptions, these companies do not steal our PII. We sell it to them, if not for a mess of pottage then at least for online services that seem to us to be free.

PII has monetary value. Maybe it is not much on an individual basis, but in the aggregate, it is worth a lot, in the billions.

If I decide that I want to buy a castle in Spain and look up the prices online, I am sure to be inundated by ads for Spanish castles. (As it is, I am swamped if I only want to visit a Spanish castle.) I could save myself the mild aggravation of seeing all those advertisements by not using a search engine, or getting driving instructions from Seville to a castle, or using social media to tell my friends about the magnificent parapets I saw, or find out the weather in the Alcazar. Perhaps there is a yak herder in the deepest depths of Siberia who is not using the Internet, but for the rest of us, the services offered on the latest apps are a part of our lives. We bought them with our PII.

So did I get appropriate value for the pittance my PII was worth? Was the benefit sufficient to reimburse me for the loss of a portion of my privacy? Do I really care if someone thinks that I am a mover and a shaker in the Spanish castle market?[10] I suppose I have reached an accommodation with the companies with which I have carried out a *de facto* transaction. And so has everyone else who uses the Internet. If you are reading this online, dear reader, you will probably receive an ad or two from ISACA®. Are you that upset?

Genuine Harm

None of the above is meant to downplay the very real and very serious consequences of genuinely harmful privacy breaches. The ease with which victimizers can find their prey on the Web is not to be dismissed. Credit card numbers are being sold; people are being stalked; politicians are illicitly swinging elections. As I write this, there is a controversy about YouTube being used by pedophiles to seek out little kids' pictures and, perhaps, the actual children themselves.[11] My point is that the latest generation of data privacy laws

> "THE EASE WITH WHICH VICTIMIZERS CAN FIND THEIR PREY ON THE WEB IS NOT TO BE DISMISSED."

should be focused on cases of actual harm, not 59,000 cases of which 58,909 were so trivial as not even to merit a fine.

Information security professionals have to implement systems and procedures to comply with the laws, however they are written. I think it is time for the community of those who work in our field and those who read the *Journal* to ensure that their work is not being used to hurt people and their legitimate interests. 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.

I will further address the notion of privacy by design in a future article.

Endnotes

1 DLA Piper, "Data Privacy Law: The Top Global Developments in 2018 and What 2019 May Bring," 23 February 2019, *https://www.dlapiper.com/en/us/insights/publications/2019/02/data-privacy-law-2018-2019/*

2 European Parliament, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, *Official Journal*, 23 November 1995, *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*

3 Office of the Privacy Commissioner of Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA), *https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/*

4 The Act on the Protection of Personal Information was updated in 2018 to align with GDPR. See DiPalo, M.; "May 30 Is Fast Approaching—Are You Ready for Compliance With the Amended Act on Protection of Personal Information in Japan?" Alston & Byrd Privacy and Cybersecurity Blog, 11 April 2017, *https://www.alstonprivacy.com/may-30-fast-approaching-ready-compliance-amended-act-protection-personal-information-japan/*

5 With the very notable exception of the United States.

6 *HIPAA Journal*, "59,000 Data Breaches Reported to GDPR Supervisory Authorities: 91 Fines Issued," 8 February 2019, *https://www.hipaajournal.com/59000-data-breaches-reported-to-gdpr-supervisory-authorities-91-fines-issued/*

7 Lovejoy, B.; "GDPR Fines Total €56M in First Year as Facebook Faces 11 Investigations," 9to5Mac, 28 May 2019, *https://9to5mac.com/2019/05/28/gdpr-fines/*

8 Satariano, 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*

9 Google is appealing the fine, so it is not clear how much they will ever actually have to pay. See Cerulus, L.; "Google to Appeal €50 Million GDPR Fine," *Politico*, 23 January 2019, *https://www.politico.eu/article/google-appeals-e50-million-gdpr-fine/*

10 For the record, I am not.

11 Fisher, M.; A. Taub; "On YouTube's Digital Playground, an Open Gate for Pedophiles," *The New York Times*, 3 June 2019, *https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html*