
3 Monroe Parkway
Suite P, #148
Lake Oswego, OR 97035

**Comments of the World Privacy Forum**
**To the Securities and Exchange Commission**
**Regarding File Number S7-11-19**

*Sent via email to rule-comments@sec.gov*

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE, Washington, DC 20549–1090

October 21, 2019

Subject: File Number S7–11–19

The World Privacy Forum is pleased to have this opportunity to comment on the SEC's proposal to modernize the description of business, legal proceedings, and risk factor disclosures that registrants are required to make pursuant to Regulation S–K. The proposal was published in the Federal Register on August 23, 2019, 84 Federal Register 44358, https://www.govinfo.gov/content/pkg/FR-2019-08-23/pdf/2019-17410.pdf.

The World Privacy Forum is a nonprofit, non-partisan 501(c)(3) public interest research group. We have testified before Congress and federal agencies regarding financial privacy and other aspects of privacy and data protection. We regularly submit comments on a wide variety of agency regulations affecting privacy and security matters. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and public comments at https://www.worldprivacyforum.org.

Our interest in the SEC's proposal to update its requirements that publicly-owned companies disclose the risk factors affecting their business is narrow. We believe that the privacy and security risks and obligations that companies face in today's complex digital environments

require that there be more disclosure of those risks. Our sole purpose in filing these comments is to request that the Commission expressly include appropriate disclosure of material privacy and security risks faced by regulated companies. As a note for clarity, our concerns about *security* in these comments relates only to the security of computers, the Internet, and comparable technologies.

We begin by asking the reader of these comments to identify the link between these companies:

- Marriott Hotels
- Equifax
- eBay
- Target
- Yahoo
- Capitol One

The answer is that each of these companies suffered a data breach involving more than 100 million records.[1] We believe that many consumers presented with this list would be able to identify the common thread in this list because the breaches received enormous publicity and because many consumers were the subjects of the data breaches and were so notified by the companies. There are additional companies with large data breaches, and securities regulators and financial industry investors would probably recognize most of the other companies that had data breaches of comparable size. We observe that counting the total number of records held by public companies that were the subject of data breaches would be like counting grains of sand on the beach. Data breaches are now a pervasive feature of modern life.

The privacy and security risks that companies face, however, are not just limited to data breaches. Other activities, some willful and some not, may also give rise to risks that are material to investors. We observe in passing the $5 Billion fine that the Federal Trade Commission seeks to impose on Facebook for its failures to comply with a privacy-related FTC consent decree. We think that amount is material on any scale. We also observe that fines under the European Union's General Data Protection Regulation can be as much as four percent of worldwide revenues.[2] That too is a material expense on any scale. We also observe that more than 130 countries around the world now have national data protection laws.[3] Although the United States does not have a comprehensive national data protection law, it still has a robust sectoral set of

---

[1] Taylor Amerding, *The biggest data breaches of the 21st century*, CSO, December 20, 2018. Available at: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[2] See Article 83, General Data Protection Regulation, http://data.europa.eu/eli/reg/2016/679/2016-05-04.

[3] Graham Greenleaf, *Global Data Privacy Laws 2019: 132 National Laws & Many Bills* (February 8, 2019). (2019) 157 Privacy Laws & Business International Report, 14-18. Available at: https://ssrn.com/abstract=3381593

privacy laws, and at the state level there, California has passed significant privacy regulation, the California Consumer Protection Act, that introduces new liabilities for companies.[4]

Fines are far from the only risks that companies face. There can be significant compliance costs from privacy and security regulation; loss of markets, customers, and opportunities; failure of business models to be consistent with privacy requirements; charges for responding to data breaches; and loss of key personnel. In the later category, we note that some corporate leaders have lost jobs in the fallout from a data breach.

In reading the SEC's proposal, we were struck by the frequent reference to environmental laws. The existing rule makes express reference to "compliance with Federal, State and local provisions which have been enacted or adopted regulating the discharge of materials into the environment, or otherwise relating to the protection of the environment, may have upon the capital expenditures, earnings and competitive position of the registrant and its subsidiaries."[5] In the 1950s, there would not have been a meaningful awareness of these risks and costs, certainly not in comparison to today's levels of awareness.[6] It was only in later decades that the environment became a subject of general concern and extensive government regulation. It became appropriate to tell companies to disclose environmental risks because of the materiality of the costs and pervasiveness of the risks.

We submit that privacy and security matters are today comparable risks for many companies. Privacy regulation, like environmental regulation, is the subject of interest and action all around the world. Every company faces some type of data risk today. We do not argue that every privacy and security risk is material to all companies, but the failure to properly address privacy and security matters is material to many companies.

Every company has personal data as one of its assets, even if that data only pertains to its own personnel. Companies falling in the latter category may have smaller risks. Other companies have extensive data on customers who purchase goods and services from them with cash or credit. A supermarket and an automobile insurer are common examples. Some companies have personal data on users who may not be customers in the traditional sense of consumers who purchase their products or services in exchange for cash. Companies providing social media platforms are examples. Some companies have personal data on consumers that forms the basis of their operations, yet they have no relationship with those consumers, and the consumers are not aware of the existence or operations of the companies. The data broker and online advertising

---

[4] California Consumer Protection Act, California Attorney General, Proposed Text for CCPA Regulations, October 2019. Available at: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf. California Attorney General, Notice of Proposed Rulemaking regarding CCPA. Available at: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf.

[5] 17 CFR § 229.101 (c)(1)(xii).

[6] See as exemplars the following: LEEDS Building Certification, ("Green" buildings). The first LEEDS building was certified in 2005. http://plus.usgbc.org/leed/. See also Ray C. Anderson, Confessions of a Radical Industrialist: Profits, people, purpose. Doing business by respecting the earth, 2009, Island Press.

industries are examples of this kind of business structure. There are many other business models that use personal data in different ways and that face difference consequences from the misuse of personal data or from new regulations about the processing of personal data.

We further observe that these are not boilerplate risks. Each industry, each company faces its own set of privacy and security risks. The preceding paragraph identifies just a few types of companies, each with its own class of risks. In some cases, new forms of regulation could expose a company to public observation and public pressure. In other cases, privacy regulation could put an end to an entire line of business that a company operates. A company that produces and sells steel to manufacturers may only face risks from the loss or misuse of employee data. A company that collects consumer data without the consent or awareness of consumers may find that privacy rules require fundamental or even existential changes in its business model. Again, there are many other types of risk faced by other companies and other industries, with significant variations on the theme.

We think that privacy and security risks are material and pervasive throughout industry today; that many companies fail to take necessary action to protect their personal data assets; and that it is appropriate for the Commission to recognize that privacy and security risks are just as important today as environmental risks were in decades past.

Our real motive is the protection of consumers and consumer privacy, but better disclosure acts to improve the health of the whole data ecosystem. If the Commission requires regulated companies to identify and disclose more about the privacy and security risks that they face, then consumers will be better off because companies will be more likely to take action to mitigate those risks. Investors will also benefit as well through a better understanding of the risks that they face when investing in public companies. We believe that, in this case, all roads lead in the same direction. Investors and consumers will benefit, each in their own way, if the Commission takes action to require companies to disclose more about the privacy and security risks that they face.

The World Privacy Forum is grateful for the opportunity to submit these comments, and we would be pleased to engage in further dialogue with you about these issues.

Respectfully submitted,

Pam Dixon,
Executive Director,
World Privacy Forum