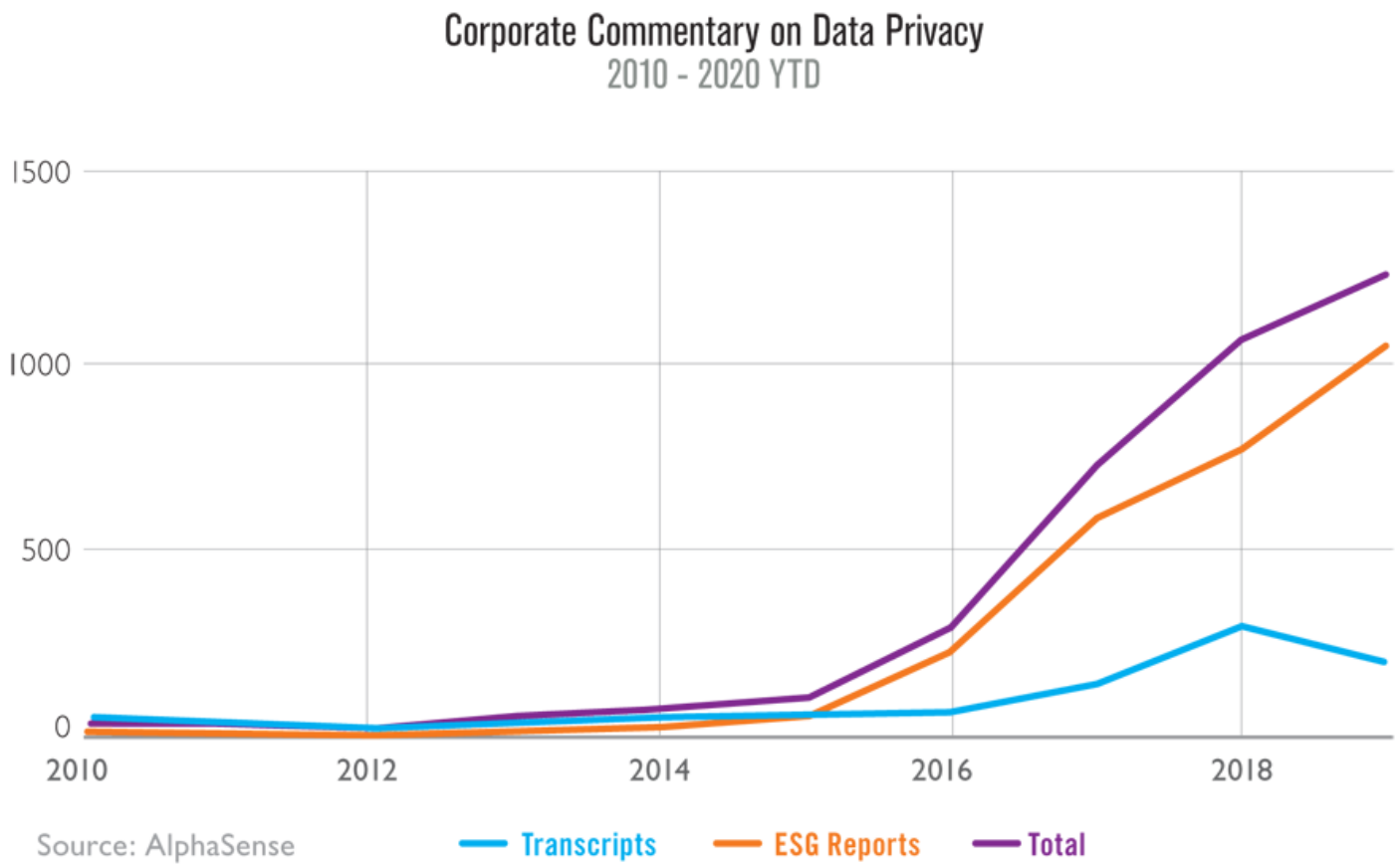
ESG and the Missing P Factor

Technology, Privacy, and eCommerce



Skeptics have opined that ESG — environmental, social, and governance, which are used to measure the sustainability and societal impact of companies — would falter in the pandemic because companies would focus on revenue streams and keeping employees healthy employees. Although companies are focusing on both, ESG remains a top priority. The perfect storm of social unrest, environmental disasters, and a global pandemic has led companies to adopt stronger ESG policies. Companies are trying to do the right thing in a challenging environment for their employees, communities, and customers.

Put another way, ESG is the measurement used to identify what companies are doing the right things. According to Bloomberg, “ESG-driven assets have now reached US$40 trillion globally, which seems to have accelerated during the pandemic.”

At the same time, privacy is becoming a prevalent concern for managing ongoing business operations with a displaced workforce. Even before COVID-19, privacy was viewed as an additional ESG metric. Some authors consider whether privacy should be added to ESG, such as PESG, and others hold that privacy is already included under “social” because it is a human rights issue, as defined by the United Nations and throughout many countries and data protection regimes.

Privacy and personal data management could also fall appropriately into social justice because of bias embedded into technology. Some argue that privacy is inherently discriminatory because only the privileged can afford it. The Sustainability Accounting Standards Board includes consumer privacy and data security under its Social Capital dimension of its framework. But does classifying

privacy under the social factor minimize privacy's impact on the sustainability and investment potential of a company?

The metrics

Just a couple of years ago, Sustainalytics (a global research company specializing in ESG), issued a report on how key major tech companies are managing privacy risk. This report reviewed the FAANG+ stock companies (Facebook, Apple, Amazon, Netflix, Google, Microsoft, and Twitter) privacy management and gross risk exposure. Few would dispute that mismanagement of personal information increases a company's exposure to data breaches, but data breaches are not limited to mismanagement. Security of personal information is an ongoing, ever-growing, and increasingly complex challenge.

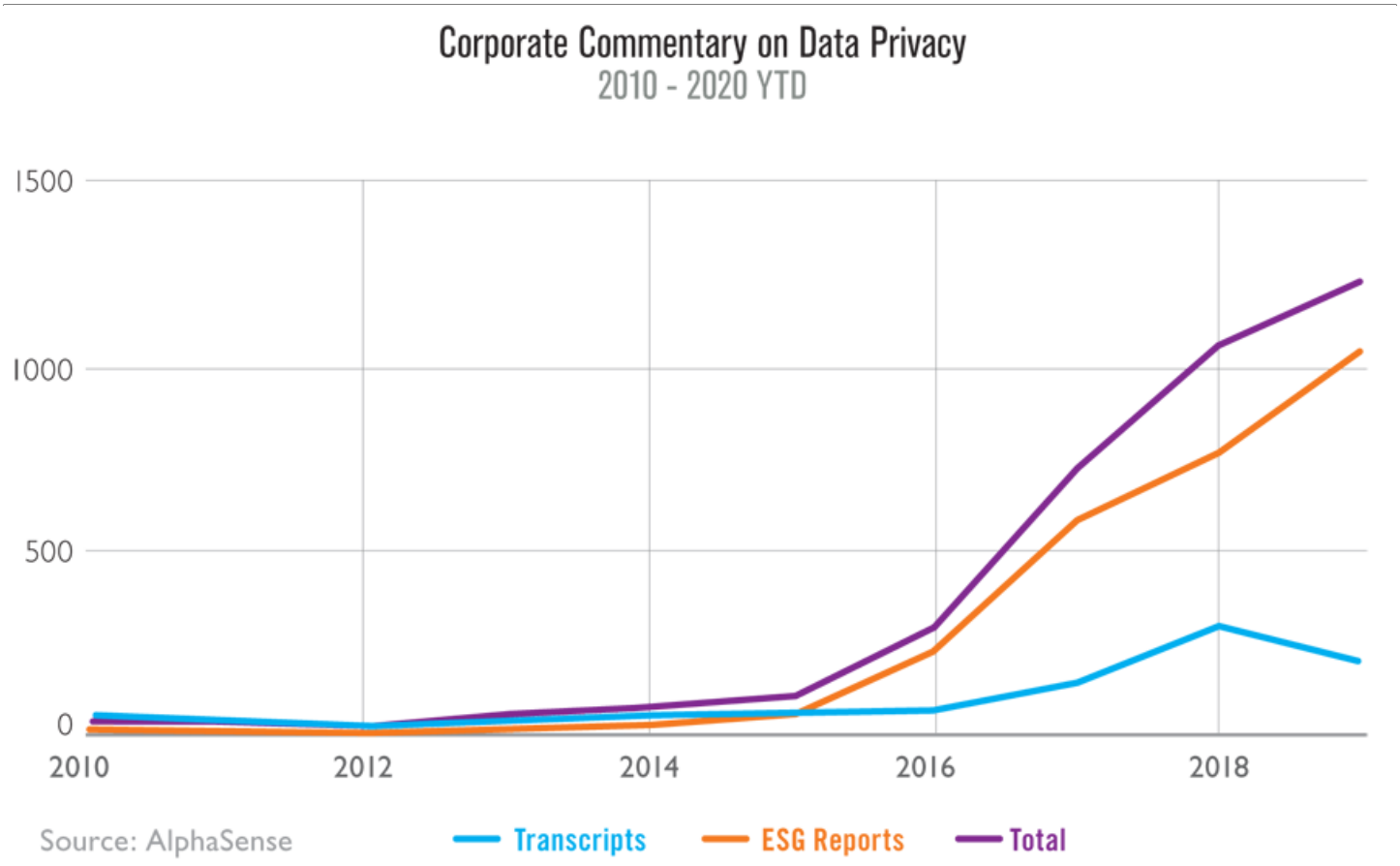
Data breaches are costly from multiple angles: mitigation, investigation, forensics, outside counsel, notifications to individuals and regulators, responses to inquiries from authorities, and more. Trust is a huge cost. Once the media focuses on the beach, brand reputation suffers.

Accenture took a different approach of measuring companies' success factors in their Competitive Agility Index. Their study found that companies who lost trust also lost an estimated US$180 billion in revenue. Although there were several factors considered in the trust measurement, management of personal data and data breaches were key considerations.

Further, RBC Global Asset Management found that the majority of institutional investors are worried about cybersecurity threats to their investments, "making it investors' foremost environmental, social, and governance (ESG) risk." This concern ranked at the top, with anti-corruption as the second highest worry. Their conclusion was that "companies that continually seek to address the growing threat of cyber attacks, and that work to effectively convey those efforts to investors, will be rewarded in a market increasingly attuned to cyber security and privacy.

Lastly, the public discourse from companies around privacy and data protection has significantly increased. AlphaSense found that in the past five years, companies' commentary, such as in their investment documents and filings along with their ESG reports, has increased a startling 920 percent.

For example, Verizon Communications Inc includes multiple areas of focus related to privacy in their most recent ESG report, such as digital safety, privacy and data protection, and cybersecurity. Verizon states that they "recognize that protecting data privacy is fundamental to maintaining the trust of [its] customers and growing [its] business." Mastercard Inc. also addresses privacy openly as a sustainability focus. These are just a couple of examples, but with an increase at 920 percent, finding examples of privacy in ESG and public statements is not uncommon nowadays.



When does the in-house counsel join?

In-house counsel play a huge role in sustainability and in privacy. The sheer amount of regulations in itself is justification, because privacy laws need lawyers to interpret them and assist the company in achieving privacy compliance. Counsel can be the privacy official, guide and advise, implement operations, and/or serve as the escalation point.

But even more importantly, ESG is a corporate strategy and culture. Executive and board of directors need to be aware and involved in ESG measures and drive. Counsel should be equally well-versed, if not more so, in the advantages and disadvantages of a robust ESG program. In-house lawyers are well positioned to analyze strategy and tactics to rapidly calculate the impact of social justice, trust, and information governance on corporate performance.

In-house counsel will realize just how critical privacy is to a company and its sustainability and attractiveness to investors.

References

[ESG Investing Looks Like Just Another Stock Bubble]

[Is there a "P" in ESG? Where does privacy fit in?]

Why Data Privacy Is an ESG Issue

Managing data privacy risk: comparing the FAANG+ stocks

Formula Won: A New Way to Measure Corporate Competitiveness

Cyber security is the top ESG concern for institutional investors

Data Privacy and Protection in the ESG Era

Verizon Privacy and data protection

K Royal

Global Chief Privacy Officer

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.