CPI TALKS…

…with Jon Leibowitz

In this month's edition of CPI Talks… we have the pleasure of speaking with Mr. Jon Leibowitz, Counsel in Davis Polk's Washington DC and New York offices. Mr. Leibowitz was Chairman of the Federal Trade Commission from 2009 through 2013 and Commissioner from 2004 to 2009.

Thank you, Mr. Leibowitz, for sharing your time for this interview with CPI.

1. You have recently stated that "Congress must pass a federal privacy law that gives consumers the choice, clarity, and enforcement they deserve." What should be the main features of this law?

First, national privacy legislation should give consumers the statutory right to control how their personal information is used and shared — including rights of access and deletion — and provide increased corporate transparency. To do so, the law should 1) require companies to solicit affirmative consumer consent before collecting sensitive data (e.g. health and financial data, Social Security numbers); and 2) allow consumers to opt out of collection of *non*-sensitive personally identifiable data. Implied consent can be permitted for certain types of company operational-use data which most consumers assume is being collected (e.g. shipping addresses, for online orders).

Second, any federal privacy requirements should be technology- and industry-neutral. In other words, companies that collect, use, and share the same kinds of covered personainformation should be subject to the same privacy requirements, rather than differing requirements based on how companies classify themselves in the marketplace.

Third, for any privacy legislation to be successful, Congress needs to ensure that the Federal Trade Commission ("FTC") has the resources to enforce the law and bring cases where necessary. To that end, the law should empower the FTC to be the primary authority to administer and enforce the new legislation. This should include the ability to impose penalties even for first-time violations, targeted APA rulemaking authority, and more resources to be able to appropriately fulfill these duties. State attorneys general will be critical allies in enforcement, and they should also be empowered to fully enforce any new federal privacy law, like they are under the Children's Online Privacy Protection Act ("COPPA").

Finally, the new federal law needs to pre-empt state laws. Americans deserve strong and consistent privacy protections no matter where they live, work, and travel — not a crazy-quilt patchwork of differing laws based on the vagaries of state legislatures. And consumers deserve to understand their rights, which militates strongly for one robust standard.

2. What would such a law learn from the experiences of the EU, and, more recently, California, in how such a law would operate in practice? What pitfalls are to be avoided?

State and regional regimes such as GDPR have shown us the promise of uniform privacy legislation across broad geographical areas. Such regimes, when at their best, can provide a more even playing field to allow for consistency and predictability in companies' compliance efforts — big and small alike — and can boost consumer confidence that their personal data is being protected.

However, due to the complexity of the privacy requirements of GDPR as it stands, large players can more easily comply with it while small players cannot.[1] Many business leaders in the EU are confused about data security concepts, like encryption.[2] EU consumers are similarly confused: only 34 percent of respondents in a survey recognized the law, and even fewer knew what it covered.[3] The EU should think carefully about the practical effects of its law, as large amounts of uncertainty may chill new business and leave consumers unsure of their own rights. In the meantime, in designing its own federal privacy legislation, the United States should avoid viewing GDPR as a default model, given that its complexity inhibits businesses' ability to implement compliance and consumers' understanding of their rights.

California's CCPA — while proving that a legislature can pass a privacy law — can be improved and strengthened at a national level. Research also shows an exceedingly high cost of compliance, with a recent study commissioned by the California Attorney General's office finding the "total cost of initial compliance with the CCPA" to be a whopping $55 billion.[4] And now, before the ink is even dry on the original CCPA regulations, a ballot initiative that passed earlier in November will create even more changes and uncertainty in the California privacy landscape.

The United States needs a powerful federal privacy law to avoid a patchwork of conflicting state requirements. Congress should focus not only on stronger safeguards for all Americans and more consumer control over data, but also on protections that are more easily understood. If consumers and businesses do not know what their rights and obligations are, the law is destined for a rocky future.

3. Opponents to a federal privacy law cite the need not to preempt "nimble privacy protections that let states meet [their] varying challenges." Is there an argument that states should be allowed to test the field before a federal law is enacted? Or do the overarching challenges of the Internet require the federal government to set common standards?

Fundamentally, it does not make sense to have 50 different state laws for consumer privacy when the very same data travels across state (and international, for that matter) boundaries. A crazy quilt patchwork of state laws is neither enforceable nor advisable. Moreover, every American deserves the same strong privacy protections no matter where she lives, works, or travels. Having one uniform set of requirements throughout the country accomplishes this and also prevents consumer and business confusion.

Notably, Attorney General Becerra — a terrific AG, and the speaker quoted above — was describing California's CCPA, which itself preempted California's own municipalities' regulations — for precisely the same reasons.

4. How do you see such a law interacting with antitrust rules? The German regulator recently issued a controversial decision (under appeal) holding a breach of EU privacy rules to constitute a breach of competition rules. Should a U.S. law contain provisions defining clearly the scope of each body of rules?

Privacy issues can sometimes overlap with antitrust — we thought a lot about when and to what extent when I was on the FTC — and a number of jurisdictions are clearly beginning to grapple with that issue. Having said that, we should all be happy if, in the next two years, the United States just passes a law that empowers consumers to control their own data. A successful federal privacy law will, like our long-standing antitrust laws, help ensure that the marketplace is free from anticompetitive and privacy-stripping business behavior that harms consumers.

---

1 Millions of Small Businesses Aren't GDPR compliant, Our Survey Finds, GDPR.eu, https://gdpr.eu/2019-small-business-survey/.

2 *Id.*

3 Kirsty Cooke, Data Shows Awareness of GDPR Is Low amongst Consumers, KANTAR, March 27, 2018, https://uk.kantar.com/public-opinion/policy/2018/data-shows-awareness-of-gdpr-is-low-amongst-consumers/.

4 California Attorney General's Office, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations" (August 2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

5. How should such a law be enforced? Should the FTC be vested with enforcement power at a federal level? Or is there a need for a separate regulator?

The FTC has been the United States' top privacy cop for the past 40 years. The biggest thing missing from its arsenal is the authority to fine first-time violators. Today, there is bipartisan support in Congress to vest the FTC with that authority, which will make the agency considerably more effective. In order to fuel the FTC's ability to enforce the new law, Congress should also grant the FTC targeted privacy rulemaking authority and significantly more resources. Fortunately, there is bipartisan support for that as well.

My view is that there is no need for a separate regulator. All too often, industry-specific regulators suffer from something called "agency capture," where an agency established to regulate a certain type of business ends up being influenced and controlled by that industry, typically to the detriment of consumers. The FTC, by having effective privacy oversight as part of a broader jurisdiction over virtually the entire economy, is somewhat more immune to that type of capture. In my view, the FTC should be the primary agency enforcing the new federal privacy law, and state attorneys general should also be empowered to enforce the law to complement the FTC's efforts.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.