*Antitrust*, Vol. 35, No. 1, Fall 2020. 

EDITORS' NOTE

# The Expanding Privacy Landscape

BY AARON BURSTEIN AND JANIS KESTENBAUM

PRIVACY ISSUES ARE ALL AROUND US. Questions from this still nascent area of law have become intertwined with many of the significant legal and public policy issues of the day. As smartphone apps are used for COVID-19 contact tracing, questions have been raised about how to balance public health and privacy. Responses to the protests that erupted in the wake of the death of George Floyd have led to questions about whether government agencies are using smartphone data to improperly identify and surveil those who attend public rallies. Personal data has long flowed freely between the United States and the European Union, but a July 2020 European court decision has threatened to make all such data transfers—and the trade that goes along with them—invalid under European law, with no clear answer about how to satisfy the court's concerns. With remote school now the norm for many children, there have been new concerns about children's privacy and security online. And as antitrust issues in the technology industry have taken center stage, questions have been raised about whether new privacy restrictions would neutralize or instead exacerbate the competition concerns that have been voiced.

The roundtable discussion featured in this issue provides an overview of many of these issues. Leading privacy lawyers from Google, the Center for Democracy and Technology, Georgetown University, and the University of Minnesota had a wide-ranging discussion about diverging views among privacy advocates on the California Consumer Privacy Rights Act (CPRA), the path forward for United States businesses in the wake of the invalidation of the U.S.-EU Privacy Shield by the Court of Justice of the European Union (CJEU) in July 2020, concerns about government surveillance of protests for racial justice, significant privacy actions by the Federal Trade Commission, and the prospects for a comprehensive federal privacy law.

Many of the articles in this issue of Antitrust take a deeper dive into these subjects. For example, in *Contact Tracing*, Robert Cattanach and Nur Ibrahim explore the wave of smartphone apps that track individuals' movements in order to notify them and others if they have encountered someone who has tested positive for the coronavirus. The authors describe the varying approaches taken across the globe to use mobile apps for contact tracing and the privacy issues raised. In some countries, such as South Korea, China, and Israel, the governments' aggressive deployment of mobile apps for contact tracing has been credited with helping to suppress the virus but has also led to concerns about government intrusion. By contrast, in the United States, contact-tracing apps have been released on a decentralized basis by a number of states on a voluntary basis with little concern about government overreach but relatively low adoption or efficacy.

Several other specific areas are rapidly changing within privacy law. For example, Ryan Mrazik and Natasha Amlani address potential changes to Section 230 of the Communications Decency Act. They explain how this longstanding statutory immunity for certain online service providers has, in just a few short years, gone from a relatively simple and settled area of law to a point of national debate, even becoming a talking point in the presidential election. The authors analyze and categorize the approaches to amending Section 230 in the current proposals in the United States and efforts to impose expanded duties on internet platforms outside the United States. Whatever course of action legislators and regulators take, Mrazik and Amlani predict that the proposed reforms have the potential to dramatically affect how individuals worldwide communicate with each other.

The theme of transformation is also at the heart of an article on the California Privacy Rights Act (CPRA) by Allaire Monticollo, Chelsea Reckell, and Emilio Cividanes, *California Privacy Landscape Changes Again with Approval of New Ballot Initiative*. Before the United States' first comprehensive consumer privacy law, the California Consumer Privacy Act (CCPA) had even gone into effect on January 1, 2020, the CCPA's architect had introduced a ballot initiative that makes far-reaching changes to the CCPA. As the authors explain, the CPRA, which California voters approved on November 3, 2020, will significantly expand the consumer rights and business obligations created by the CCPA. In addition, the CPRA mandates the creation of a new state agency to implement and administratively enforce the CPRA. While businesses have two years to get ready for the new law, most of which goes into effect on January 1, 2023, the authors explain that this will demand substantial effort by affected businesses, even those that are already compliant with the EU General Data Protection Regulation (GDPR).

This issue also provides a view of significant privacy developments outside the United States and some of their interactions with antitrust law. Wei Han and Cunzhen

*Aaron Burstein is a partner at Kelley Drye & Warren LLP in Washington, DC. He counsels clients on privacy and data use issues in compliance, transactional, and investigative settings. Janis Kestenbaum is a partner at Perkins Coie LLP in the Privacy & Data Security practice in Washington, DC. Burstein and Kestenbaum were the Issue Editors for the privacy theme portion of this issue.*

Huang describe the privacy and cybersecurity laws that govern China's 900 million internet users. Noteworthy enforcement actions include a sweep by China's four main regulators that examined the terms and user experiences of more than 1000 apps and an investigation by the Ministry of Industry and Information Technology's Network Security Bureau of the face-swapping app ZAO for allegedly collecting excessive personal information. On the antitrust front, China's Anti-Monopoly Law, Anti-Unfair Competition Law, and other legal authorities have been used in a few cases involving personal data practices, but Han and Huang note that China's overall approach to addressing data practices through competition law has been "cautious" and is still subject to vigorous debate.

Europe continues to be at the forefront of questions about the intersection of privacy and competition. Florian Haus discusses how Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU) may apply to personal data processing in the context of joint and unilateral conduct, respectively. With regard to joint conduct, Haus discusses the possibility that competitors' contributions to joint databases could create economies of scale, leading to broader and deeper data sets, better products and services at lower costs—and thus benefit consumers in a way that justifies competitors' cooperation. Where a single firm's dominance is concerned, Haus discusses the German Federal Cartel Office's (FCO) action against Facebook under TFEU Section 102 and Germany's domestic antitrust law. The FCO alleged that Facebook abused its dominance in social networking by requiring users to consent to data collection on non-Facebook sites. On appeal, the Federal Supreme Court sided with the FCO and, in Haus's view, embraced the proposition that antitrust "is relevant to what can be legitimately agreed in a contract"—at least when a dominant firm collects a broader range of data than is necessary to provide its services.

Looking back at the first two years of GDPR implementation, Emily Jones highlights some of the key practical lessons that have emerged from initial enforcement actions and court decisions. Transparency and consent remain challenging issues, particularly where the use of website cookies (and similar technologies) is concerned. The CJEU and Member State supervisory authorities have made it clear that the standard for consent under the GDPR—"freely given, specific, informed and unambiguous"—is stringent, and companies need to be able to demonstrate that they obtain such consent when they rely on it as a basis to set cookies. Other evolving areas under the GDPR include accountability and the ability to demonstrate compliance with the Regulation; data security; joint controllership; and the exercise of data subject rights, e.g., the right to access personal data held by a data controller. Companies must adapt to these standards while at the same time managing uncertainty in cross-border data transfer requirements in light of the CJEU's invalidation of Privacy Shield and the Court's concerns about the other main data transfer mechanism, standard contractual clauses: "In one fell swoop, many businesses have had the mechanism they used for data transfers (Privacy Shield) declared invalid and another (standard contractual clauses) needing additional assessments and possible supplementary measures."

Finally, two articles take a deeper look at a fundamental question: When do privacy concerns become antitrust concerns?

Garrett Glasgow and Chris Stomberg examine this question through the lens of consumer welfare. Drawing on sources that relate personal data processing and data breach risks to consumer harm, Glasgow and Stomberg note that there are steep challenges in quantifying how consumers value privacy and how they make trade-offs between privacy and the benefits of providing personal data in exchange for services. Privacy signals are typically far less clear than price signals, or, as the authors state, "We cannot tell if people are overpaying in terms of their privacy if we do not know the price they have paid." Uncertainty in the value of privacy carries over to the formulation of remedies. Glasgow and Stomberg analyze whether reducing the "price" of a service by constraining its ability to collect and process personal data could reduce the quality of the service, drive away users, and ultimately reduce consumer welfare.

John Harkrider urges caution in applying George Akerlof's theory of markets for lemons—which holds that markets may fail when consumers lack sufficient information to distinguish good products from bad—to privacy. Harkrider notes that the challenges are both empirical and legal when it comes to applying Akerlof's theory to the acquisition or maintenance of monopoly power through privacy misrepresentations. Legally, plaintiffs asserting that privacy misrepresentations are an exclusionary act face an "extraordinarily high bar" for proving that, but for the deception, consumers would have turned to a competitor. Empirically, Harkrider points to several services that grew quickly to challenge large platforms as reasons to be skeptical that large bases of user data—even if acquired through misrepresentation— present a significant barrier to entry. The GDPR and CCPA could, in Harkrider's view, make it more difficult for such challengers to emerge.

This issue's view of privacy developments in the United States and beyond and privacy's relation to antitrust, though sweeping, is far from comprehensive. Changes in the U.S. political landscape, the continuing evolution of privacy regulations around the world, and the growing attention to data flows and privacy as trade and national security issues will be areas to watch in the months and years ahead. ■

*For readers interested in additional information and ongoing engagement on privacy and data security issues, the Antitrust Law Section's Privacy and Information Security Committee (PRIS) offers a wide variety of programming and resources on the privacy issues addressed in this issue, and many others. For more information, go to https://www.americanbar.org/groups/antitrust_law/committees/committee-pris/.*