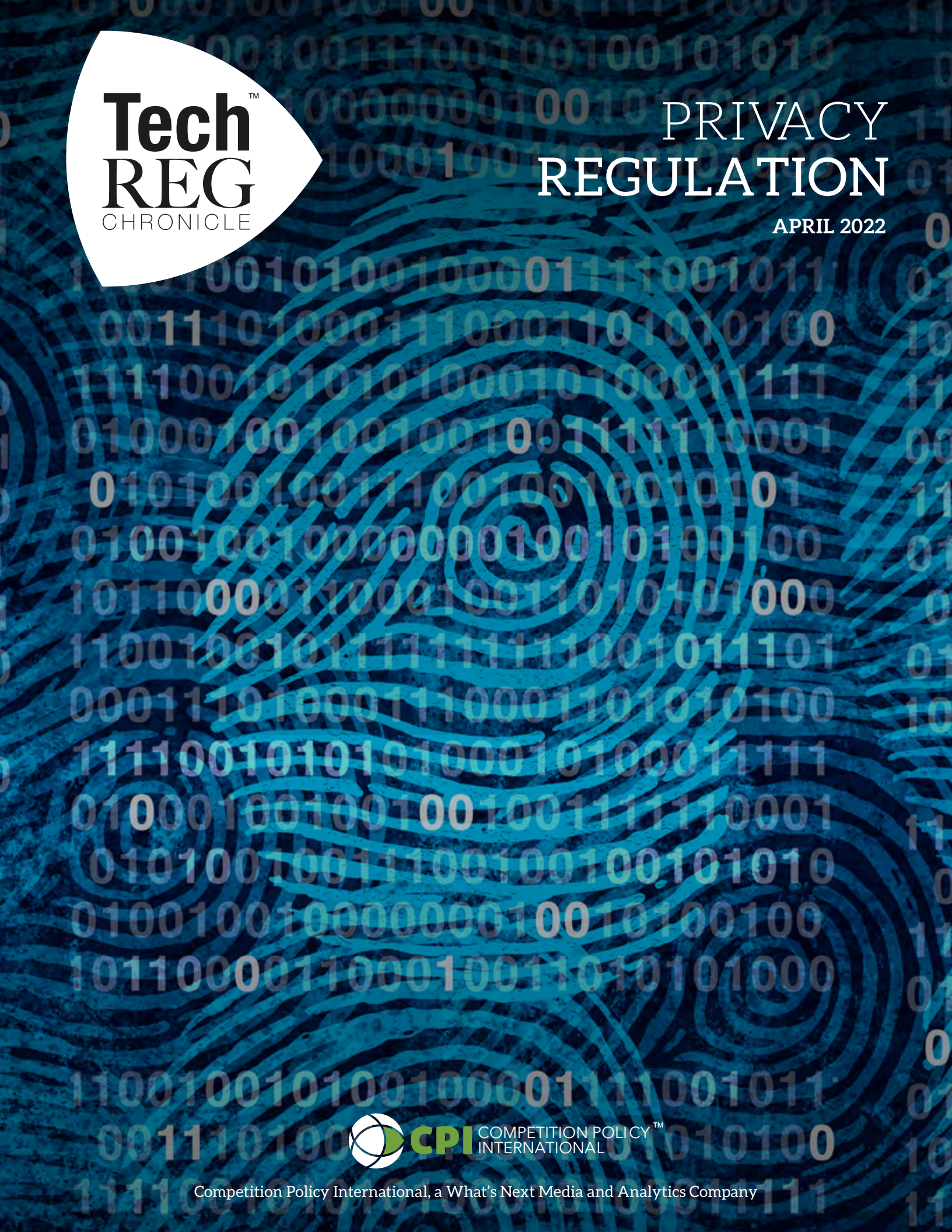


Tech REG CHRONICLE

PRIVACY REGULATION

APRIL 2022

CPI COMPETITION POLICY INTERNATIONAL

Competition Policy International, a What's Next Media and Analytics Company

LETTER FROM THE EDITOR

Dear Readers,

Privacy is one of the key policy issues of our time. The shift to a digital economy has brought about fundamental changes to the nature of modern commerce. Many of the most valuable services used by citizens worldwide are free at the point of consumption. Search, social media, messaging, and various forms of online content are available to users for no up-front monetary charge. Instead, companies monetize such services through other means, typically by selling advertising.

This renders the consumer's quid-pro-quo (or the "price" they pay) not to be counted in Euros, dollars, or cents, but in terms of their attention (or "eyeballs" in marketing jargon). Companies increasingly rely on data concerning user behavior and preferences in order to better target the advertisements that generate their revenue.

This shift raises legal challenges. Antitrust, in particular, has long been governed by the implicit motto that price competition is the central nervous system of the economy. When price is no longer quantifiable in currency terms, the application of established principles becomes challenging. Other concerns relating to breaches of privacy have led to different legislative developments, including notably the European Union's General Data Protection Regulation. That law became a template for similar legislation around the world, including in jurisdictions as diverse as Turkey, Mauritius, Chile, Japan, Brazil, South Korea, South Africa, Argentina, and Kenya. As of 2022, even the United Kingdom retains the law in identical form despite no longer being an EU member state. The California Consumer Privacy Act ("CCPA"), adopted in June 2018, follows a similar schema.

The pieces in this Chronicle address various aspects of the regulation of privacy and personal data in the modern digital economy, including how this nascent (and rapidly evolving) field can and should interact with other domains of economic law (notably antitrust).

CPI COMPETITION POLICY™ INTERNATIONAL

Kirk J. Nahra provides an overview of U.S. privacy law in its current state of flux. In the absence of legislation at the Federal level, the piece projects the development of an array of new "comprehensive" state laws, creating some new privacy protections while imposing compliance challenges on industry. As the article outlines, privacy regulation is undergoing constant change at this moment in time, creating a range of challenges and opportunities for regulators, legislators and private entities.

Melanie Drayton & Brent Homan outline the work of the Digital Citizen and Consumer Working Group ("DCCWG"), an international body under the auspices of the Global Privacy Agency. The DCCWG is focused on considering the interactions between privacy, consumer protection and competition bodies. The article explores some of the key learnings of the DCCWG over the past 5 years. Ultimately, the DCCWG view is that collaboration between competition agencies and privacy agencies is imperative to achieve coherent regulation of the digital economy.

Dr. Paul Voigt & Daniel Tolks outline the framework of the proposed EU Data Governance Act ("DGA"). The DGA is intended to create conditions to enable a European single market for data, notably by strengthening trust in key players and to boost cross-sector data sharing. Naturally, the topics addressed by the DGA are therefore diverse, and include the re-use of data held by public sector bodies, data intermediation services, data altruism, and the creation of a European Data Innovation Board. This article provides a useful primer for any reader seeking to track the evolution of European data regulation.

Anne C. Witt outlines the issues at stake in Case C-252/21 Facebook Inc. and Others v. Bundeskartellamt. The key question facing the German Courts is the extent to which competition agencies should be allowed to consider the legality of certain conduct under the GDPR when applying competition rules. The piece argues that in the age of data-based business models, it is unhelpful to look at competition and privacy issues in isolation. Judicious regulation of digital platforms requires an interdisciplinary and interinstitutional approach.

Ben Rossen explores the options open to the U.S. FTC to regulate privacy in the absence of Federal legislation covering the field. The FTC is widely expected to commence a rulemaking process to "curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination." The paper addresses some of the reasons why FTC rulemaking may be a poor substitute for federal legislation (and potentially an inefficient allocation of limited agency resources).

Finally, **Melissa J. Krasnow** outlines the implications of the FTC's Final Rule regarding Standards for Safeguarding Customer Information. The article also highlights differences between the FTC Rule and the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies. Financial institutions to which the FTC Rule applies must assess the extent to which their information security programs satisfy the those requirements. By contrast, others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law/.

In sum, this Chronicle provides a fascinating snapshot of the current state of privacy regulation worldwide. As the pieces should make evident, the implications of growing privacy concerns will have numerous impacts on different aspects of economic regulation, including notably the enforcement of the antitrust rules.
As always, many thanks to our great panel of authors.

Sincerely,
CPI Team

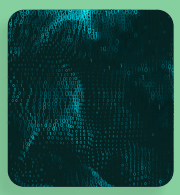
TABLE OF CONTENTS

CPI COMPETITION POLICY™ INTERNATIONAL

PRIVACY REGULATION

APRIL 2022

SUMMARIES



THE FUTURE OF PRIVACY REGULATION

By Kirk J. Nahra

U.S. privacy law is undergoing dramatic change on an accelerating pace. New laws across the country address specific industries, certain kinds of data, and various concerning practices. There is international pressure to improve the state of U.S. privacy law. At the same time, technological progress also is accelerating, leading to more personal information being gathered in more places by more entities. The essay reviews the current state of U.S. privacy law and how these changes may play out in the near future. We expect to see a continuing array of new "comprehensive" state laws, creating some new privacy protections while imposing new compliance challenges on industry. We are seeing regulators at both the state and federal levels explore creative new enforcement approaches, while navigating meaningful limits on their authority. We are seeing the U.S. Congress struggle to find a role in this overall debate, as there has been little movement on a national privacy law. All in all, privacy law is undergoing almost constant change at this moment in time, creating a broad range of challenges and opportunities for regulators, legislators and entities of all shapes and sizes.

REGULATING THE DIGITAL ECONOMY – WHY PRIVACY AND COMPETITION AUTHORITIES SHOULD TALK TO EACH OTHER

By Melanie Drayton & Brent Homan

Data sits at the center of our digital economy and does not conform to regulatory or geographical boundaries. It is clear further understanding and collaboration by authorities across privacy, consumer protection and competition regulatory spheres is needed to achieve optimal regulatory outcomes. The Digital Citizen and Consumer Working Group ("DCCWG") is focused on considering the intersections of, and promoting regulatory co-operation between, the privacy, consumer protection and competition (also referred to as antitrust) regulatory spheres. In doing this, the DCCWG seeks to support "a global regulatory environment with clear and consistently high standards of data protection, as digitalisation continues at pace." This article explores some of the key learnings of the DCCWG over the past 5 years. Ultimately, the DCCWG view is that collaboration between competition agencies and privacy agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation.

THE RIGHT TO PRIVACY AND PERSONAL DATA: SOME CONSIDERATIONS FOR OPTIMAL PROTECTION

By Blanca Lilia Ibarra Cadena

The protection of privacy and personal data is a must for maintaining democracies and avoiding authoritarianism led by extreme surveillance. For the optimal protection of both rights, it is necessary to promote regulatory compliance, ethics, self-regulation, the strengthening of regulations, and of public bodies and institutions.

"FIRST ACT" OF THE EUROPEAN DATA ECONOMY – THE DATA GOVERNANCE ACT

By Dr. Paul Voigt & Daniel Tolks

Large amounts of data are the core of the digital transformation. According to current estimates, the global volume of data will increase by 530 percent between 2018 and 2025. This includes not only personal data, but also and in particular non-personal data, for example from industrially deployed sensors which constantly capture production data. The European Union has recognized the potential of these – today largely untapped – data sources and is striving to promote the exploitation of this data on the one hand and to uphold European values and principles, in particular data protection and fair competition, on the other. To this end, a number of data-related measures are to be adopted as part of the European Strategy for Data. The most developed measure to date is the Data Governance Act ("DGA"), which is about to be implemented by the European Parliament. The DGA is intended to create fundamental framework conditions for the European single market for data and to strengthen trust in certain key players in order to facilitate and boost cross-sector data sharing between companies, consumers and public bodies. Consequently, the topics addressed by the DGA are diverse, including the re-use of data held by public sector bodies, data intermediation services, data altruism, and the creation of a European Data Innovation Board. It is therefore worth taking a closer look at the final draft and having an initial assessment of the proposed measures.

FACEBOOK v. BUNDESKARTELLAMT – MAY EUROPEAN COMPETITION AGENCIES APPLY THE GDPR?

By Anne C. Witt

The relationship between privacy and competition law is complex and contentious. May or should competition agencies consider business conduct's negative impact on privacy when this effect was the consequence of a restriction or absence of competition? This contribution critically assesses the issues at stake in Case C-252/21 *Facebook Inc. and Others v. Bundeskartellamt*. It argues that competition agencies should be allowed to consider the legality of business conduct under the GDPR when applying competition law. In the age of data-based business models, it is unhelpful to look at competition and privacy issues in isolation. Judicious regulation of digital platforms requires an interdisciplinary and interinstitutional approach.

THE FTC SAFEGUARDS RULE: INFORMATION SECURITY PROGRAM ELEMENTS

By Melissa J. Krasnow

This article describes the elements of an information security program under the Federal Trade Commission Final Rule regarding Standards for Safeguarding Customer Information (the "FTC Rule"). While the effective date of the FTC Rule was January 10, 2022, certain information security program elements become effective as of December 9, 2022. This article also highlights differences between the FTC Rule information security program elements with counterparts under the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies. Financial institutions to which the FTC Rule applies should assess the extent to which their information security programs satisfy the elements of an information security program under the FTC Rule, identify, and address any gaps and document the foregoing. Others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law requirements for information security programs.

CAN THE FTC PROMULGATE EFFECTIVE PRIVACY RULES?

By Ben Rossen

In the absence of federal privacy legislation, the FTC is widely expected to commence a rulemaking to "curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination." This paper addresses some of the reasons why FTC rulemaking is a poor substitute for federal legislation and an inefficient allocation of limited agency resources. While the FTC has considerable power to craft rules banning unfair or deceptive practices, Magnuson-Moss rulemaking is slow and resource-intensive, may not produce enforceable final rules, and does not necessarily preempt inconsistent state law. Plus, the limits of FTC's unfairness authority do not always square well with privacy. Competition rulemaking, meanwhile, would be a terrible strategic blunder for the FTC and should be avoided. The FTC should instead focus its efforts on the most egregious practices that plainly fit within the statutory rubric of unfairness.

THE FUTURE OF PRIVACY REGULATION

BY

KIRK J. NAHRA

Kirk J. Nahra is a Partner with WilmerHale in Washington, D.C., where he co-chairs the Cybersecurity and Privacy Practice. He teaches Health Care Privacy and Security Law and Information Privacy Law at the Washington College of Law at American University. He is an adjunct professor at Case Western Reserve University Law School and the University of Maine Law School. He also serves as a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis and as a fellow with the Institute for Critical Infrastructure Technology. He received the 2021 Vanguard Award from the International Association of Privacy Professionals (IAPP, awarded in recognition of exceptional leadership, knowledge and creativity in privacy and data protection. https://iapp.org/news/a/kirk-nahra-receives-2021-iapp-vanguard-award/ He can be reached at kirk.nahra@wilmerhale.com and follow him on Twitter @kirkjnahrawork.

01 INTRODUCTION

Not to be too technical about it, but privacy law in the United States is a bit of a mess. While, unlike the European Union, the United States does not have a single dominant privacy law, we instead have dozens, maybe hundreds. This morass of different laws and regulations, at the state, federal and even municipal levels, creates enormous compliance challenges and has led to the development of an entire large industry of privacy professionals.[2] Yet, in the eyes of much of the world and much of the privacy advocacy community, our U.S. privacy law is insufficiently protective of individual privacy interests. This essay looks at the future of privacy regulation and how it may play out over the next decade.

2 I am a proud member of the International Association of Privacy Professionals, which has grown to include more than 75,000 members around the world. https://iapp.org/.

02
OUR CURRENT U.S. PRIVACY LAW

A. Specific Laws Covering Specific Things

Much existing U.S. privacy law has been opportunistic. We have a law protecting privacy interests in video rental records because of a newspaper article involving the video rental history of a judicial nominee. We have the Drivers Privacy Protection Act because of the tragic shooting of a young actress. We have the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule because of congressional concerns about the portability of health insurance coverage when individuals left one employer for another when they had pre-existing medical conditions. And the Gramm-Leach Bliley Act ("GLB") privacy provisions exist because of the consolidation of the financial services industry promoted by the rest of the GLB law.

This pattern has continued, leading to core U.S. privacy law being driven today by three categories of laws:

- Those dealing with particular industry sectors (e.g. health care, financial services, education);
- Those dealing with particular kinds of data (biometrics laws, children's data, facial recognition restrictions); or
- Those dealing with particular practices (CAN-SPAM for email marketing and TCPA for telephone and texting communications).

The result of this set of provisions is a legal hodgepodge, with different data and different people being regulated in different ways, with overlaps and conflicts and significant gaps. This is the current primary path of U.S. privacy law. It provides substantial protections in some settings, very limited protections in others, and no direct protection for large segments of the U.S. economy not directly regulated by any of the laws.[3]

B. "Comprehensive" State Laws

A recent addition to this set of U.S. laws is the "comprehensive" state privacy law. This story begins with the California Consumer Privacy Act ("CCPA"). CCPA has an interesting and so far unique history, driven by the California referendum practice and the resulting "gun to the head" need to pass a privacy law very quickly (with not surprising resulting drafting flaws). It also – despite the history – has had a disproportionate impact on U.S. privacy law. The CCPA already has been amended directly several times, and now has been largely overhauled through the California Privacy Rights Act. To date (recognizing that this statement may be changing in real time) two other states have joined this category – Virginia and Colorado (although this expansion beyond California has been slower than many expected). Numerous other states have introduced laws on these issues, including at least a dozen already in 2022 (as of this writing). We expect these laws will continue to move forward in states across the country.

These laws generally purport to be "comprehensive" – but none so far really are. CCPA, for example, is primarily a large gap-filling law. It exempts meaningful swaths of the data universe – including (essentially) any entity or data regulated by other laws (such as HIPAA or GLB), most employee data and all data from non-profits. If you aren't dealing with employee data, aren't a non-profit, are big enough, and aren't subject to other privacy laws, you likely are covered by CCPA.

Where it applies the CCPA is primarily a law that creates new opportunities for individuals to exercise rights. CCPA provides these new rights (such as improved access rights and the "do not sell" opportunity), but imposes few obligations on the front end on companies subject to the law. This means that there is an affirmative burden on consumers to exercise these rights. The Virginia and Colorado laws are loosely similar, but each has their own variations. New proposals in other states continue to explore new directions, and no single model has yet emerged.

03
INTERNATIONAL DEVELOPMENTS

U.S. privacy law is not developing in a geographic vacuum. More and more countries around the world are implementing their own privacy standards. Where these laws exist, they tend to be more protective of individual privacy than U.S. law generally and more comprehensive in their application. The General Data Protection Regulation in Europe, for example, applies (essentially) to all personal data held by an entity operating in Europe or otherwise subject to these laws through its business activities (without the kinds of exemptions that apply in CCPA). GDPR

3 Companies falling in these gaps do need to be concerned with enforcement activity, from the Federal Trade Commission and state Attorneys General (at least), in connection with data breaches or data practices impacting consumer protection concerns.

has created substantial compliance obligations for U.S. companies subject to it – which is many companies with any meaningful international footprint. China, India and many other countries are adding their own variations to the international regime. At the same time, an additional development has been increasing concerns in European courts about protections applicable to personal data that is transferred to the U.S. from Europe – with these concerns creating real time risks of broad scale shutting down of these transfers.

04
THE FUTURE OF U.S. PRIVACY LAW

With this background, where do we go from here?

A. An Increasing Volume "Comprehensive" State Laws

It seems clear that, in the short term, additional states will pass "CCPA-like" laws. These laws will provide some additional level of protection for some data that currently falls into regulatory gaps. While following all of the current proposals seems challenging, none of the current laws (yet) fundamentally change the approach of CCPA, even if the key elements often are slightly different. A Massachusetts proposal – which one leading privacy academic called the "most revolutionary" proposal - already has been significantly watered down in committee. Some state laws include a private right of action provision, which certainly would alter the remainder of the debate. At the same time, as these state laws add, one by one, new requirements that are similar but not identical, the compliance complexities continue to grow.

B. A Dominant FTC Privacy Regulation

The Federal Trade Commission – the primary "default" U.S. privacy regulator at the federal level – continues to explore means of increasing privacy regulation in the interest of consumer protection. The FTC, under Section 5 of the FTC Act, has authority to take action against certain "unfair and deceptive" practices. Generally, misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices and are thus prohibited by Section 5(a) of the FTC Act. Also, acts or practices are deemed unfair under Section 5 of the FTC Act if they cause, or are likely to cause, substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or the competition.

Starting with the *BJ's Wholesale*[4] case from 2005, in a series of close to 100 cases, the FTC has brought enforcement actions that have defined a law of data security under a "reasonable and appropriate" standard. This success was defined – in part – by the fact that most of its cases (and all of its early cases) were negotiated settlements without court challenge. Once court challenges came – mainly in the *Wyndham*[5] and *LabMD*[6] cases – the scope of the FTC's actions in this area, while not cut off, clearly were limited and the underpinning legal support for these actions fell into question. In the privacy area, where there is no current clear approach to what would make a privacy practice "unfair," it is clear that the FTC would face an uphill battle under its current regulatory and statutory authority.

Accordingly, the FTC is setting off on a long path to develop a privacy regulation that would define unfair practices. Because the FTC Act does not provide for regulations, the FTC is forced to use the cumbersome Magnuson-Moss approach to its rulemaking, which is expected to take close to five years, if it can get off the ground at all. These efforts appear to be based both on a desire to pressure Congress to act in the privacy area and to develop a fallback effort if Congress does not succeed with a national privacy law. While current FTC leadership is interested in pushing the boundaries of its current authority, this path is one potential avenue for developing national standards. If the FTC is successful with this approach – clearly an uphill battle – Congress may feel relieved of pressure to pass a national privacy law.

"Starting with the BJ's Wholesale case from 2005, in a series of close to 100 cases, the FTC has brought enforcement actions that have defined a law of data security under a "reasonable and appropriate" standard

4 *In the matter of BJ's Wholesale Club, Inc.*, available at https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter (2005).

5 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

6 *LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018).

C. A "Comprehensive" U.S. Privacy Law

The potential gold standard (perhaps for both consumers and industry) may be a U.S. national privacy law. Congress has been debating a national privacy law since the mid-1990s, with little meaningful progress and lots of noise. With competing pressures today from ongoing privacy and security "scandals" (insufficient pressure so far); growing challenges from the obligations and vagaries of a growing number of state laws (likely meaningful pressure), and critical challenges from abroad related to data transfers (real pressure), there is a reasonable possibility of a national privacy law in the next several years. This law could help define appropriate best practices and reasonable enforcement, and could balance good privacy protection with appropriate protections for beneficial data practices. That is both possible and a meaningful challenge.

What are the key issues for a national law? Currently, two issues dominate the national conversation: preemption and a private right of action.

Preemption would involve the question of whether the state privacy laws would continue in effect, or would be replaced by a national law. There are meaningful benefits to both industry and (in some instances) to consumers from a clear and defining national standard that does not require 50 state variations. As consumer and industry groups look for a middle ground on preemption, I expect that (1) the complexity of compliance with each new state law will be a meaningful reason for industry to push for a national standard; (2) this push will not be maintained if there is no preemption; and (3) the baseline level for consumer protections in a national privacy law grows with each new state law. Look for some kind of compromise on this issue that will incorporate the key provisions of state laws that have been passed to date (along perhaps with a time limit on preemption) as well as a role for state Attorneys General in enforcement.

There are similar challenges in connection with a private right of action. Will consumers have a right to sue for (some or all?) violations of this national privacy law. There has been a meaningful debate in the courts and academia about the principles that should support a consumer's general right to sue for damages as a result of a data breach. This debate is in no way resolved. We would expect an even greater set of cases to be filed if there is a national private right of action. Are there meaningful options for compromise here? The CCPA includes a "right to cure" before lawsuits can be filed. Can there be heightened pleading standards? A defined set of issues that would permit suit for some violations but not others? A compromise here can be developed, but there may be somewhat less room for a middle ground. Perhaps an expanded role for State AGs can address both the preemption and private cause of action issues.

"Preemption would involve the question of whether the state privacy laws would continue in effect, or would be replaced by a national law

Beyond these top two issues, there is a long array of critical "second tier" issues that likely will define the actual success of a national privacy law. Here are some key issues for consideration:

- How will the national privacy law deal with existing federal laws?
- Who will enforce the national privacy law (essentially a question of the FTC or a new national data protection agency modeled on EU data protection agencies)
- Will the national law be "rights driven," as many of the state laws have been, or will it set specific standards for companies independent of a consumer's actions?
- Will there be a single privacy standard (as with GDPR) or will the law attempt to address different kinds of data on different ways?
- Will there be sensitive categories of data with additional protections?
- How will the law address (if at all) artificial intelligence and algorithmic discrimination issues? (critically important issues that may not directly raise privacy concerns even though there clearly is a meaningful impact on consumers from how these formulas are applied)
- Will the law be able to address the concerns of international regulators and courts so that a global standard can emerge?
- Will the law include data security practices?
- Will the law create a national data breach notification standard (which only would be useful if it preempts state law, since (unlike the privacy area) all states have data breach notice laws?

05 RECOMMENDATIONS

We are a long ways away from a national privacy law at this point, and there are a significant number of questions that need to be answered before an effective law can be passed. At the same time, there are growing pressures for such a law (and I expect industry to increasingly favor a law as more and more states pass their own versions). I have some recommendations.

A national law that preempts state law. As a practicing lawyer in this area for the entirety of privacy being an issue for law firms and their clients, I have seen first-hand the challenges of navigating conflicting and overlapping laws, for different industries and data. While I am happy to be a professional beneficiary of this complexity, the resources spent on understanding and applying these complex provisions – presuming good faith efforts at compliance – do not benefit either industry or consumers. A clear single standard will help both consumers and industry if it provides sufficient consumer protections. A national law that preempts state law while meeting or exceeding the standards of the current state laws can do both.

Meaningful enforcement authority. The FTC Act generally does not provide the FTC with the opportunity for monetary penalties in the first instance. It is hard to see a national privacy law that would provide sufficient consumer protections without creating this right to monetary and other remedies. Congress should consider both the scope of these monetary remedies and other means of relief that also will create pressures on companies to comply and not just view enforcement as a cost of doing business.

While other countries have created specific privacy regulators to enforce privacy laws, in most instances they did not previously have an "FTC like" regulatory agency. Rather than creating a new agency, a strengthened FTC with clearer enforcement standards likely can meet consumer protection goals while providing industry with appropriate guidance and obtainable standards.

The states can play an important role in privacy enforcement, even under a national privacy law. Giving the state attorney general a viable role seems like a good solution to both the preemption and private cause of action issues, and, if appropriately defined, may encourage a reasonable compromise on all of these grounds. Providing specific limitations on how states can exercise this authority is important, as should some kind of coordination requirement with the FTC (to avoid some of the "pile-ons" that occur today).

The role for regulation. An effective national privacy law needs to address a large volume of highly complicated issues. It is certainly reasonable to question Congress' ability to navigate all of these issues in a way that both leads to the passage of a law and that addresses these issues in effective ways. I would support a relatively "bare bones" national privacy law, and a clear delegation to the enforcement agency (the FTC or otherwise) to draft regulations that develop the detail of this array of complex issues. We have some experience with this concept working. In the health care context, the Department of Health and Human Services was tasked with preparing privacy and security regulations under HIPAA – without any meaningful substantive guidance from Congress on any of the core issues other than who could be covered by the rules. Over roughly 20 years of development, we have seen these rules generally work in ways that are appropriate for both consumers and industry, and that allow significant privacy protections in an environment that still permits an effective health care system. It isn't perfect, but its pretty good. As with data security protections, perfection should not be the standard. This experience provides some useful and perhaps hopeful guidance on how a federal privacy regulation might fare.

> *An effective national privacy law needs to address a large volume of highly complicated issues*

Addressing kinds of data. GDPR in Europe is the prototype of a "one size fits all" privacy provision. It applies to all data in virtually all contexts. There are slight modifications for sensitive data. At the same time, GDPR includes little of the nuance that makes some U.S. laws so effective (with HIPAA as a leading example). This may be the most challenging issue for the actual substance of a national privacy law. The HIPAA rules, for example, include a number of key provisions that are designed specifically to balance appropriate privacy protection with steps to facilitate the effective operation of the health care system, which is good not only for the health care industry but also for patients – who want a reasonable cost health care system that does its job well. But this generally effective nuance of the HIPAA rules comes at the expense of having wide gaps in coverage for "non-HIPAA health data," (a result of how Congress could define who was covered by the law), along with meaningful challenges as large volumes of data elements that are not at all about your health now seem useful for health related purposes. The current system – even for health care rules that generally work well (where they apply) - now is being faced with growing challenges as the system evolves and we

learn more about how health care works. I do not expect Congress to be able to handle this level of subtlety. Whether the law will try to attempt these variations – through legislation or appropriate regulation – is a significant open issue.

Specific consumer protections. The current set of state laws focus on consumer rights. These laws expand on the traditional idea of "notice and choice" as a leading element of privacy law. Increasingly, however, it seems clear that this notice and choice model has failed. Consumers simply cannot be expected to navigate privacy notices and choices from hundreds or thousands of data collectors in real time and in settings where consumers cannot possibly have full knowledge of what their choices mean. A more targeted choice model in some ways puts even more burden on consumers.

Accordingly, U.S. law should include specific defined responsibilities for companies, independent of consumer rights. These rights to choose and other consumer rights should supplement baseline standards rather than be the primary set of standards. I have advocated for a "context-based" set of rules.[7] Professors Neil Richards & Woodrow Hartzog support a "duty of loyalty" standard.[8] However defined, an appropriately consumer – protective privacy law should define behavior for companies independent of consumer actions.

The challenge going forward — if Congress chooses to define these appropriate uses and disclosures rather than rely primarily on notice and choice — is how to define the appropriate context for all industries and all purposes, or to find some other means of developing a standard that can be applied to such a wide range of activities, encompassing health care, financial services, retail, social media, education, employment, and the broad, and perhaps unlimited, range of other categories of users of personal data.

Add on Elements. There are core issues that need to be addressed in any national privacy law. There also are a variety of possible add-on topics that could be addressed (and that sometimes are addressed in other laws in this category). Data security requirements could be included – but likely should be addressed primarily through regulation rather than through detailed legislative requirements. A national data breach notification law that preempted state standards would be useful to streamline the differing state requirements, but is not critical because all state currently have notification laws.

> *"Accordingly, U.S. law should include specific defined responsibilities for companies, independent of consumer rights*

The questions involving artificial intelligence are more complicated. Clearly, there are realistic consumer risks in this area that need to be addressed. At the same time, many of these issues are not directly privacy issues, nor have they historically been addressed through privacy laws. Instead, these kinds of discrimination risks typically have been addressed in other substantive areas. Given the challenges that Congress will have on these issues, incorporating a sophisticated approach to artificial intelligence seems destined to both bog down the progress of a privacy law and likely to lead to an ineffective result.

06 CONCLUSION

Privacy law has grown from a set of principles that defined rights of individuals against the government, to a growing and increasingly complicated set of rules (largely in the past 20 years) that define various practice of companies and their consumers during the Internet era. The law is developing quickly, but technology clearly is moving even faster. Personal data is increasingly important to a growing range of activities, some good and some much less good. Lawyers in virtually all fields should understand at least the basics of privacy law.[9] A wide range of other professionals will need to understand and apply these evolving principles across a growing range of companies. This business need is occurring whether or not we have new kinds of privacy law, and consumer risks (and some benefits) are growing at the same time.

We can expect meaningful developments in this field for the foreseeable future. At the same time, there is a growing recognition of the costs – both economic and personal – of a system that provides uneven and inconsistent protec-

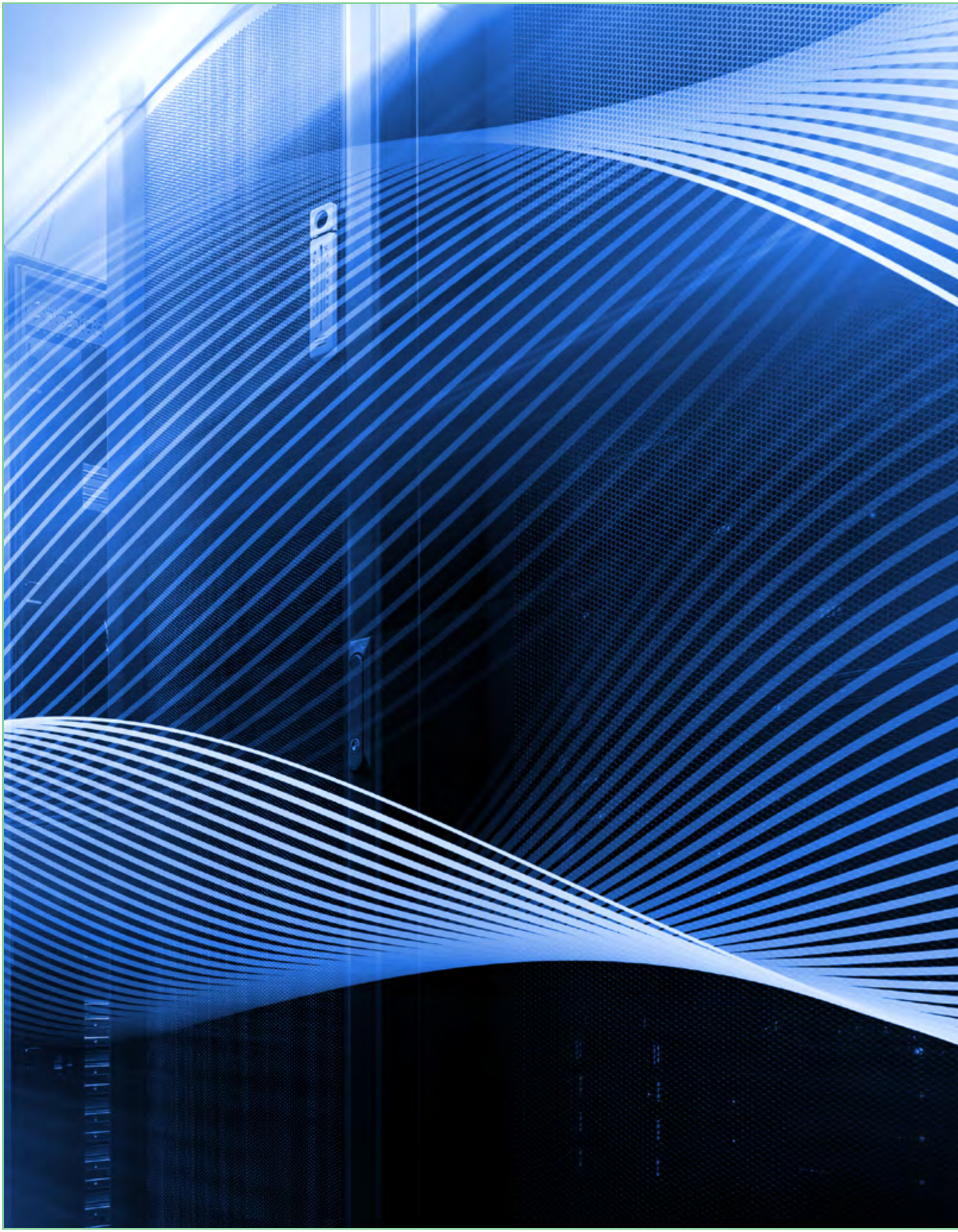
7 Kirk J. Nahra & Lydia Lichlyter, Federal Privacy Legislation Should Be Context-Sensitive, LAW360 (February 27, 2020), available at https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20200227-federal-privacy-legislation-should-be-context-sensitive.

8 Richards & Hartzog, "A Duty of Loyalty for Privacy Law," 99 Washington University Law Review (forthcoming 2021).

9 See Nahra, "Privacy Law and the First-Year Law School Curriculum," 23 GREEN BAG 2D 21 (Autumn 2019).

tions, and often may provide little or no realistic protection for consumers at all. How these issues will be resolved will impact how companies operate - and how consumer rights and interests will be protected - in a wide range of industries for a growing range of practices around the world.

> *Privacy law has grown from a set of principles that defined rights of individuals against the government, to a growing and increasingly complicated set of rules (largely in the past 20 years) that define various practice of companies and their consumers during the Internet era*



REGULATING THE DIGITAL ECONOMY – WHY PRIVACY AND COMPETITION AUTHORITIES SHOULD TALK TO EACH OTHER

BY MELANIE DRAYTON

& BRENT HOMAN

Acting Deputy Commissioner, Office of the Australian Information Commissioner and Co-chair of the Global Privacy Assembly Digital Citizen and Consumer Working Group.

Deputy Commissioner, Compliance, Office of the Privacy Commissioner of Canada and Co-chair of the Global Privacy Assembly Digital Citizen and Consumer Working Group.

01 INTRODUCTION

Data sits at the center of our digital economy and does not conform to regulatory or geographical boundaries. It is clear further understanding and collaboration by authorities across privacy, consumer protection and competition regulatory spheres is needed to achieve optimal regulatory outcomes. In recognition of this, the Global Privacy Assembly established the Digital Citizen and Consumer Working Group ("DCCWG"), which is focused on considering the intersections of, and promoting regulatory co-operation between, the

privacy, consumer protection and competition (also referred to as antitrust) regulatory spheres.[2] In doing this, the DCCWG seeks to support "a global regulatory environment with clear and consistently high standards of data protection, as digitalization continues at pace."[3] This article explores some of the key learnings of the DCCWG over the past 5 years and competitive outcomes.

> ***Data sits at the center of our digital economy and does not conform to regulatory or geographical boundaries***

The increasing intersection between privacy and competition is rooted in the digital economy and its growth and innovation. The emergence and morphing of data-driven business models has led to value being extracted from data more successfully than ever, and being made available on an unprecedented level, not only to dominant, global social and commercial enterprises, but also to small and medium-sized businesses. As the digital economy continues to evolve from the bricks and mortar world, so too have the competitive implications arising from the conduct of its players.

Where privacy and consumer protection regulation are more naturally aligned, the same cannot always be said for the privacy and competition regulatory spheres. Accordingly, in recent years, the DCCWG has placed a greater focus on the intersection of privacy and competition in order to better understand how authorities from both regulatory spheres are approaching this intersection and ultimately leverage that understanding in advocating for greater collaboration between competition and privacy regulators. To do so, the DCCWG launched the recently completed privacy and competition "Deep Dive."

Comprised of two complementary reports, which can be found in the DCCWG's 2021 Annual Report,[4] the Deep Dive brings together both the theory and practical application underpinning our current understanding of this intersection.

The first is a DCCWG-commissioned independent academic report by Professor Erika Douglas of Temple University Beasley School of Law, titled "*Digital Crossroads: The Intersection of Competition Law and Data Privacy*" (the "Digital Crossroads Report").[5] The Digital Crossroads Report is the first of its kind to delve comprehensively into the intersection between competition and privacy. For this report, Douglas reviewed more than 200 publicly available, English-language materials related to antitrust and data privacy agencies around the world. It provides a detailed overview of the current regulatory landscape, highlights compliments and tensions between philosophies at the center of these two regulatory spheres and underlines its emerging development as an important cross-regulatory challenge requiring further consensus-building and international collaboration.

The second is the DCCWG-authored '*Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration*" (the "Interview Report").[6]

The Interview Report was based on a series of interviews with competition authorities from around the globe, and identifies key takeaways, potential synchronicity between regulatory spheres as well as obstacles to be surmounted and possible tensions to be mitigated. Perhaps most importantly, the Interview Report also includes multiple practical examples that illustrate how collaboration and communication across regulatory spheres can serve to improve outcomes for global citizens. Through collaboration there exists an opportunity to leverage cross-regulatory complements and mitigate tensions, and move towards finding a balance without sacrificing the objectives of either regulatory regime. Cross-regulatory collaboration reveals the required synchronization between competition and privacy agencies to support a robust digital economy that engenders consumer trust in privacy protections and competitive markets. In this sense, collaboration between competition agencies and privacy agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation.

With this in mind, this article will explore some of the key findings from those Deep Dive reports, and what this means for the increasing intersection between privacy and com-

2 Given the cross-jurisdictional nature of this work, we have used competition and antitrust, as well as "privacy" and "data protection," interchangeably in this article, while noting of course the terminology is context specific.

3 Global Privacy Assembly, 43rd Closed Session Res, *Strategic Plan 2021-2023* (October 2021), https://globalprivacyassembly.org/wp-content/uploads/2021/10/2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf.

4 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *2021 Annual Report* (August 2021),. https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3h-version-4.0-Digital-Citizen-and-Consumer-Working-Group-adopted.pdf.

5 Erika Douglas, Digital Crossroads: The Intersection of Competition Law and Data Privacy (Temple University Legal Studies Research Paper No. 2021-40, July 6, 2021)., https://ssrn.com/abstract=3880737 or http://dx.doi.org/10.2139/ssrn.3880737.

6 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1.

petition. This article will first explore both the tensions and shared objectives of these regulatory spheres. It will then outline future opportunities towards a shared understanding. Finally, it will provide some practical insights shared from regulators across the globe, on what it is to co-operate and collaborate across regulatory spheres.

02
TENSIONS AND SHARED OBJECTIVES

As Douglas noted in the Digital Crossroads Report, the interactions between regulatory spheres are nascent, varied and complex. Despite these intersections often being described as complementary, the relationship between antitrust law and privacy is often more nuanced and complex.[7] Accordingly, Douglas emphasizes the need to bring context to our understanding of how privacy and competition interact with each other as we begin to develop theory, shared understanding, and practice in this area. Recognizing

The first part in building this shared understanding is considering the legal framing of privacy and competition rights and interests, and the different legislative objectives of privacy and competition spheres. Taking this comparative approach highlighted that both privacy and antitrust/competition law vary by jurisdiction. For example, in the European Union and its member states, data privacy has its foundation as a constitutionally protected right. In contrast, in the United States, data privacy law, at least at the federal level, is a sub-category of consumer protection law. Jurisdictions such as Canada and Australia take a more principles-based approach, rather than conceptualizing privacy in terms of rights.[8]

Furthermore, there is often a different terminology used across jurisdictions. For example, while privacy authorities conceive the term "personal data" as directly relating to protections and sensitivity, competition authorities are more focused on the "data" aspect in the term, particularly in how datasets containing both personal and non-personal data contribute to a company's market power. This reflection was reinforced by the DCCWG's Interview Report, where we found that privacy and competition authorities speak different regulatory languages with varied interpretations of certain concepts.[9]

Data protection legislation and antitrust legislation also have different objectives. While data protection law is primarily focused on the privacy interests of individuals, the main objective of antitrust law is to promote economic consumer welfare. As Douglas noted, privacy law "exists as a growing collection of rights and interests related to personal data access, portability, correction, deletion, transparency of processing and minimizing data collection."[10] The conceptual differences between these regulatory spheres "presents an 'apples to oranges' reconciliation between the fundamental human right of privacy, and the economic interests advanced by competition law."[11]

Not surprisingly, jurisdictions which are more focused on economic efficiency in their competition law are less likely to incorporate privacy considerations into their competition analysis. On the other hand, jurisdictions which have broader antitrust goals – including fairness and the provision of equitable opportunities for business – have greater scope for including privacy considerations in their competition analysis.[12]

"The first part in building this shared understanding is considering the legal framing of privacy and competition rights and interests, and the different legislative objectives of privacy and competition spheres

Despite these differences in the objectives between the regimes, there are also common policy interests. For example, both antitrust and privacy law seek to promote consumer trust in digital markets, see data portability as

7 Douglas, *supra* note 6, at 1.

8 *Id.* at 5.

9 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1.

10 Douglas, *supra* note 6, at 31.

11 *Id.* at 33.

12 *Id.* at 6.

beneficial and seek to encourage and maintain consumer choice.[13] This again points to the value in enhanced collaboration between privacy and competition authorities to work towards these common policy interests.

03
TOWARDS NEW UNDERSTANDING

As identified by Douglas, the current leading theory of the intersection between these areas of law argues that antitrust law should consider privacy only when privacy is a parameter of product (or service) quality that is affected by competition (the "privacy-as quality" theory).[14] The prevalence of the privacy-as-quality theory is illustrated by the fact that it also appears in the Interview Report as the "traditionalist approach to regulation." Regardless of the name, the central elements of this theory remains the same – privacy will be taken into consideration when it is a competitive factor, and set aside when it is not.

In our (the DCCWG) view, the growing incidence of privacy as a non-price factor in competitive assessments, represents an opportunity, if not necessity, for greater collaboration – even with adherents to this "traditionalist" regulatory approach. While this is arguably an oversimplification, a core tenant of competition theory is that a consolidation of market power increases the likelihood of increased prices which is generally bad for competition. Where privacy is a non-price factor of competition, the inverse likely holds true in that a consolidation of market power increases the likelihood of reduced privacy protections – either because companies no longer feel the need to compete on privacy and reduce their efforts in that area, or because consumers have few privacy related alternatives to choose from – which is bad for privacy.

As the Digital Crossroads Report notes, the implications of the privacy-as-quality theory are still at an early stage, and there are likely to be challenges to its application. For example, how can and should privacy as a non-price factor be considered in competition analysis? How do competition authorities view privacy harms when they are unrelated to competition? How can the differences in consumer preferences to privacy be accounted for? Because this theory has predominantly been applied to merger reviews, "[i]t is not yet clear how the concept of privacy as quality might be applied across other areas of antitrust law, such as market definition, market power or cartels."[15] However, as discussed in both the Digital Crossroads Report and the Interview Report, this also represents an opportunity for greater cross-regulatory collaboration in the future. As we (privacy authorities) enjoy a comparative advantage in our understanding of how certain privacy functions operate, we may be able to assist competition authorities improve the level of statistical confidence in their competitive analyses.

For example, privacy authorities are likely to help further the discussion around the concept of the "Privacy Paradox" – which proposes that while individuals claim to value their privacy, their actions suggest otherwise. The idea of the Privacy Paradox complicating efforts to assign a weight to privacy as a non-price competitive factor is discussed at length in the Interview Report. In fact, one of the competition authorities interviewed questioned whether it "might really be a by-product of a corporations' lack of privacy engagement with individuals, as opposed to the expression of an individual preference (or lack thereof)."[16] While the cause of the Privacy Paradox is up for debate, we (the DCCWG) would suggest that it may be rooted in part in a misunderstanding about what privacy actually means, as some incorrectly equate privacy with secrecy, rather than *control* over one's personal information, and how/when individuals choose to share it.

> ***As the Digital Crossroads Report notes, the implications of the privacy-as-quality theory are still at an early stage, and there are likely to be challenges to its application***

Finally, privacy protections are beginning to be cited as a justification for anticompetitive conduct. Both reports analyze the Toronto Real Estate Board's unsuccessful attempt to cite compliance with Canada's private sector privacy legislation as a justification for what the courts found to be

13 *Id.* at 7.

14 *Id.* at 62-63.

15 *Id.* at 64.

16 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1, at 21.

anti-competitive conduct.[17] As this trend is likely to continue, sharing our privacy expertise will help competition authorities understand whether a company's actions truly serve a privacy related purpose, whether that company is over-interpreting their privacy obligations, or if they are simply using privacy as an excuse.

This presents a significant opportunity for collaboration between data privacy and antitrust authorities to work to develop these analytical tools for measuring the competition-related effects on privacy quality. Accordingly, there is value in deepening that cross-doctrinal understanding and agency cooperation so that enforcement or policy in one area does not unnecessarily undermine the achievements or goals in the other area of enforcement. The shared interests of antitrust and data privacy enforcers can be reinforced to advance their interests.

04
PRACTICAL PERSPECTIVES

Through our ongoing intersection work, as well as the Interview Report, the DCCWG sought to understand how competition authorities are practically approaching privacy and data considerations when carrying out their antitrust analyses, and leverage the views and examples provided in advocating for greater collaboration between competition and privacy regulators. Perhaps most importantly, the Interview Report (a product of interviews with 12 competition authorities around the globe) also includes multiple practical examples that illustrate how competition regulators have successfully incorporated privacy considerations into their enforcement work and through cross-regulatory collaboration or consideration, found the balance between the two without sacrificing the objectives of either. The benefits of such collaboration are superior outcomes that holistically serve a robust digital economy along with individuals' privacy rights and consumer interests.

The interviews highlighted that there are already many practical examples of regulatory cross-collaboration to date, including:

i. the creation of cross-regulatory forums (e.g. the UK's *Digital Regulation Cooperation Forum* ("DRCF") and the Australian *Digital Platform Regulators Forum* ("DP-REG")),

ii. the application of privacy considerations to anti-trust cases (e.g. the German Bundeskartellamt Facebook case, the Competition and Consumer Commission of Singapore's ("CCCS") merger and abuse of dominance guidelines, the United States' Federal Trade Commission's finding on the Google/DoubleClick merger and the European Commission consideration of the Facebook/WhatsApp merger), and

iii. the incorporation of privacy considerations into competition remedies (Colombia *Superintendencia de Industria y Comercio* ("SIC") remedy for a banking joint venture).

The UK's DRCF[18] was formed in July 2020 with the overarching goal for participating authorities to better respond to the scale and global nature of large digital platforms and the speed at which they innovate. The DRCF is comprised of the United Kingdom's Competition and Markets Authority, the Information Commissioner's Office, the Office of Communications (or Ofcom) and the Financial Conduct Authority. It is a prime example of how authorities can increase cross-regulatory cooperation, while fulfilling their respective enforcement mandates, via strategic and formalized network engagement.[19]

> ***"The UK's DRCF was formed in July 2020 with the overarching goal for participating authorities to better respond to the scale and global nature of large digital platforms and the speed at which they innovate***

Last month, in March 2022, a collaborative regulator network was established in Australia. The DP-REG' brings together the Australian Communications and Media Authority, the Australian Competition and Consumer Commission, the Office of the Australian Information Commissioner, and the Office of the eSafety Commissioner to support a streamlined and cohesive approach to the regulation of digital

17 Douglas, *supra* note 6, at 126-130; and Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1, at 26 & 27.

18 Competition and Markets Authority, The Digital Regulation Cooperation Forum, March 10, 2021 (UK) https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

19 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, at Annex 1, at 20.

platforms.[20] This network is an initiative to consider and collaborate around issues of regulating digital platforms with respect to competition, consumer privacy and data regulation, as well focusing on the intersections with online safety issues.

The DCCWG also found that there have been practical examples of applying privacy considerations in competition cases. For example, in the German Bundeskartellamt ("BKartA") Facebook case, BKartA found that Facebook's terms of service, and the manner and extent to which it collects and uses data, amounted to an abuse of dominance. In assessing the appropriateness of Facebook's behavior under competition law, the BKartA took the violation of European data protection rules to the detriment of users into consideration Where the BKaratA has applied privacy considerations to a single enforcement matter, the CCCS has laid the ground work to apply them to future enforcement matters. As part of a public consultation on proposed amendments to various enforcement guidelines, the CCCS has explicitly stated that, where appropriate, their merger assessments will treat data protection as an aspect of quality. Another proposed amendment identified the control/ownership of data as a possible determinant of market power with respect to abuse of dominance assessments.

"The DCCWG also found that there have been practical examples of applying privacy considerations in competition cases

As a practical example of competition agencies incorporating privacy considerations into their competition remedies, the Interview Report presented the SIC's "Banks" recommendations to the Superintendencia Financiera de Colombia (Colombia's financial regulator) the SIC's T was asked to assess the creation of a new digital joint banking venture. between Colombia's three largest banks It is worth noting that the SIC has multiple enforcement mandates, including consumer protection, privacy and competition. Despite the competitive nature of the assessment, several of the SIC's recommendations were privacy orientated, including ensuring data was treated in compliance with Colombia's privacy laws, obtaining consent, and allowing for data portability.[21] These practical examples demonstrated the way in which authorities are taking a progressive and proactive approach to considering how privacy and data are factored in antitrust analyses, as the intersection between these two spheres inevitably increases in the digital economy.

05 CONCLUSION

The recent work of the DCCWG, both in commissioning the Digital Crossroads Report and conducting interviews with regulatory authorities resulting in the Interview Report highlighted three consistent key themes.

Firstly, in the digital economy there has been a dramatic expansion in how the privacy and antitrust areas of law interact in digital environments.

Secondly, the theory and understanding in this intersection is still at a very early stage. While there is some emerging consensus, there is still work to be done to build understanding of not only where the intersections are complementary, but where they are not aligned. In this sense, it is essential to deepen our understanding of competition and privacy trade-offs. We need to understand where there are potential trade-offs between the promotion of competition and the protection of privacy in law enforcement and policy, and whether and to what extent such trade-offs are likely to occur.

Thirdly, both of these reports highlight that collaboration between privacy agencies and competition agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation. There are complex questions which need addressing, including how to measure the effects of competition on privacy or vice versa. We need to be asking when and how the quality of privacy protection in a market is likely to be affected by competition. There are many ways in which we can promote cross-regulatory collaboration, including domestic engagement between privacy and competition regulators, participating in global networks for cross-regulatory collaboration and advocating for domestic and international legislative vehicles to remove existing barriers and facility cross-regulatory collaboration.

Privacy and competition regulation will continue to intersect, and there will be continued shared goals and areas of tensions as we navigate these spaces. In our research,

20 Digital Platform Regulators Forum (DP-REG), DP-REG joint public statement, March 11, 2022 https://www.acma.gov.au/dp-reg-joint-public-statement.

21 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, at Annex 1, at 28-29.

the DCCWG saw examples and cases where, notwithstanding the existence of tensions between regulatory objectives, consultation and cooperation can result in an outcome that satisfies both objectives, rather than sacrificing either. Regulatory collaboration has the potential to ensure that each regulatory sphere's objectives are advanced.

> ***Privacy and competition regulation will continue to intersect, and there will be continued shared goals and areas of tensions as we navigate these spaces***

THE RIGHT TO PRIVACY AND PERSONAL DATA: SOME CONSIDERATIONS FOR OPTIMAL PROTECTION

BY
BLANCA LILIA IBARRA CADENA

President Commissioner of National Institute for Transparency, Access to Information and Personal Data Protection (INAI México), Chair authority of the Global Privacy Assembly

01 INTRODUCTION

Privacy is the key to the most intimate details of our lives. We do not want to disclose certain information without our consent. In turn, privacy entails the protection of personal data. Safeguarding both rights is a must for maintaining liberal democracies and avoiding authoritarianism led by extreme surveillance from both private and public corporations.[2]

Personal data has acquired a high value in the current economic system. Such value "is not based on the data but rather on its manage-

2 Vélis, Carissa. (2021) "*Privacidad es poder*" (Privacy is Power) p. 98.

ment, use, and relationship to other data."[3] This situation has caused large and medium-sized technology companies to profit from the overuse of personal data to predict users' behavioral patterns.[4]

There has been a broad discussion about social media, disruptive technologies, and the ongoing surveillance we all experience. I would first like to state a clear stance: I am not against technology and innovation; on the contrary, I am in favor of progress. I am aware that technological advances form a key part of the development and progress in areas as critical as medicine and personal safety. In Mexico, many people use social media daily. For example, according to the 17th Study on Users' Internet Habits in Mexico, by the Internet Association MX ("AIMX"), in 2020, there were 84.1 million Internet users in Mexico, representing 72 percent of the population.[5] However, it is worth questioning how online services work, particularly in light of their surveillance over user habits, behaviors, and data. This should be done admitting that there are risks, and working to improve the protection of users' rights and freedoms.

Many have led us to believe that modernity and progress mean implementing disruptive technologies to automate everything. In contrast, the idea of progress implies both the enhancement and improvement of knowledge and the material advancement of humanity; it also implies moral evolution.[6] We can contribute to such development in all these aspects by guaranteeing people's fundamental rights and strengthening democratic institutions.

"Many have led us to believe that modernity and progress mean implementing disruptive technologies to automate everything

Scientific and technological innovation is critical for the State's development, provided it is ethical and aimed at a more equitable and just society.

Multiple news items have emerged in recent years concerning unethical practices engaged in by international corporations such as Cambridge Analytica. Recently, much public attention was focused on the statements by Frances Haugen (the Facebook whistleblower), who claimed that the company had promoted misinformation to gain economic benefits.[7] In addition, she reported an in-house study carried out by the company that confirms that the Instagram platform is harmful to children and adolescents because it exacerbates certain psychological conditions. Despite the above, we continue to use these platforms. We have become dependent on them and justify their use in the name of efficiency.

As you may recall, as early as 1890, in the United States, jurists Warren and Brandeis had already established criteria for the right to privacy in the face of technological advances. In 1973, the United States put in place the "Fair Information Practice Principles" ("FIPPs"). In 1970, European countries started enforcing personal data protection regulations, Germany being the pioneer in this regard. Moreover, various supranational instruments acknowledge the general principles in this area using varying approaches. The Universal Declaration of Human Rights of 1948 and the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data represent the first supranational instruments regulating the right to data protection. Subsequently, there was the Council of Europe Convention on the Protection of Individuals concerning Automated Processing of Personal Data of January 1981, among other instruments.

The above examples show that the principles of privacy are not new. However, much has been written of late, criticizing the law for not being sufficient to protect the public from the dangers of technological advances. Nonetheless, we never ask ourselves if developers are up to the task of building new technologies for the good of modern societies while still respecting the rights and freedoms of individuals. Therefore, it is necessary to consider whether technological advances must comply with the principles that are - and were - already established in international recommendations and guidelines.

3 Mendoza Enríquez, Olivia A. (2018). "*Marco jurídico de la PDP en las empresas de servicios establecidas en* México: *desafíos y cumplimiento"* {PDP "Legal Framework for service provider companies in Mexico: challenges and compliance"}. Revista IUS, volumen 12, no. 41, p. 269. Available at http://www.scielo.org.mx/scielo.php?pid=S1870-21472018000100267&script=sci_arttext (viewed on March 13, 2022).

4 *Ibíd*.

5 Asociación de Internet MX, *17° Estudio sobre los Hábitos de los Usuarios de Internet en* México 2021 (17th Study on the Users' Internet Habits in Mexico, *2021*). Available at: https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Ha%CC%81bitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v16%20Publica.pdf, viewed on March 13, 2022.

6 Castillo Aguirre, Jesús. "*La evolución histórica de la idea de progreso en el contexto del desarrollo regional*," (Historical evolution of progress under a regional development framework), p. 380, available at https://www.redalyc.org/pdf/2631/263141553047.pdf.

7 Interview for the "60 Minutes - TV Show" *60 minutes.* Available at https://youtu.be/_Lx5VmAdZSI.

In the current context, it appears that neither legislation nor self-regulation have been capable of orienting the behavior of organizations towards respecting the rights to privacy and personal data protection ("PDP"). Thus, unethical decision-making has always been present, although it grew shortly after the creation of Google, the pioneer of surveillance capitalism.[8]

Despite the above, I believe it is possible to get back on the right track for technological and market development respecting privacy and PDP. To this end, it is crucial to make ethical decisions in the interest of the common good and to comply with the general principles governing the matter, and, in general, focus on respect for fundamental rights.

02
REGULATORY COMPLIANCE, ETHICS, AND SELF-REGULATION: THE VIRTUOUS TRIANGLE

To ensure that organizations and governments conduct their actions focusing on respect for human rights, we should consider three issues: first, compliance with regulations, whether they come from national or international legislation, as these incorporate principles of our concern that are crucial for safeguarding the rights. Undoubtedly, we should add ethics (recently incorporated into certain formal legislation in terms of ethical compliance). As the last cornerstone of the virtuous triangle for developing new information and communication technologies that are functional and respectful of privacy and the right to PDP, we have the implementation of self-regulation mechanisms.

Below, I will explain each point of the so-called virtuous triangle for adequately protecting the rights to PDP and privacy.

A. Regulatory Compliance

Regulatory compliance refers to abiding by legislation or conventional frameworks, and it is by nature mandatory. In case of non-compliance by corporations, they should be declared illegal and penalized.

Rules are based on guiding principles, establishing duties and rights. Therefore, compliance is the minimum basis for an organization to operate under an established regime.

Companies and organizations must understand that principles of respect for privacy have been in effect since 1948 and are updated through legislation, conventions, and international guidelines. [9] A country that has agreed on the matter in data processing must likewise comply with such principles, even in the absence of sound regulations throughout the State.

Regarding the principles of PDP and privacy, specifically on technological development, I consider the principle of privacy by design and by default to be transcendental. Therefore, privacy must come first before implementing technologies, systems, and functions, and especially when implementing artificial intelligence, big data, and virtual reality. The same is true for business operations, physical architectures, and network infrastructure, which are becoming fundamental for companies and governments to automate processes and tasks.

According to the former Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian,[10] in broad terms, this principle consists of integrating the guarantee of privacy into the core of the technology or system architecture. In other words, it seeks to ensure that confidentiality is set up by default, which means that thorough prior planning is required.

The principle of privacy by design and by default is a way to integrate and comply with the general principles before technology implementation, a protectionist approach to fundamental rights, which, I reiterate, is what is needed today

In addition to the above, an instrument is vital, together with the principle of privacy by design and default, to achieve controlled technology development or intensive data processing. These are known as PDP Impact Assessments ("PDPIAs").

8 Zuboff, Shoshana, *La era del capitalismo de la vigilancia*. (The Era of Surveillance Capitalism), México, Paidós, p. 23.

9 The Universal Declaration of Human Rights of 1948 refers only to respect for private life.

10 Cavoukian, Ann. Privacy by Design, The 7 Foundational Principles. Available at http://jpaulgibson.synology.me/ETHICS4EU-Brick-Smart-Pills-TeacherWebSite/SecondaryMaterial/pdfs/CavoukianETAL09.pdf. Viewed on March 15, 2022.

Under the EU General Data Protection Regulation (Article 35),[11] the person in charge of data processing must analyze PDPIAs in the light of new technologies. Their nature, scope, context, or purposes may pose a high risk to personal data owners. This duty must be fulfilled before data processing. Thus, in my opinion, these assessments document the implementation of the privacy principle by design and default.

B. Ethics and Ethical Compliance

Ethics refers to "a model of a person or community's virtuous life and lived values, embodied in their practices and institutions."[12] This behavior includes professional practice. In companies, we usually call it company philosophy and are the mission, vision, values, and objectives that give it meaning. Therefore, we can say that organizations have ethics.[13]

Ethics stem from good or bad behavior. In this sense, Fernando Navarro García, Director of the Ethics and Corporate Social Responsibility Study Institute (*Instituto de Estudios para la* Ética *y la Responsabilidad Social de las Organizaciones*), points out that "*ethics [help] to forge (good) character through prudent, mediated and reflected decision-making.*" Thus, it is crucial to ponder their consequences for organizations and their stakeholders.[14]

Ethical corporations build legitimate confidence and security in society. Thus, on this topic, we cannot overlook ethics.

> ***Ethics refers to "a model of a person or community's virtuous life and lived values, embodied in their practices and institutions***

Ethics must be demonstrated and reflected in commitments, although reinforced through actions. Currently, we have seen that rules control ethical compliance. For example, the main goal of EU Directive 2019/1939 on compliance is to set up a standardized legal framework for European Union countries. This framework will ensure protection and anonymity for employees and those reporting possible infringements, breaches, or fraudulent actions in organizations. To this end, companies must implement proper approaches and procedures for complaints.

I think this is excellent practice, although we should ask ourselves why something done purely out of free will, such as ethics, had to be regulated. Are corporations ethical?

Some best practices that are proper to point out for ethical compliance are the following:

- To develop Codes of Ethics.
- To set up Ethical Committees to discuss how to proceed and the decision-making process.
- To encourage the role of *compliance officers* (not only in the criminal field but in *compliance* in general).
- To set up complaint mechanisms due to unethical behaviors.
- To implement straightforward procedures for the anonymous file of complaints and use of mechanisms.

In this regard, compliance with PDP principles is closely related to ethics. Organizations should consider it a capital gain since this builds up trust and legitimacy among users in a win-win environment. It is by far more profitable to be an ethical company that proactively complies with regulation in the long run.

C. Self-regulation

Self-regulation refers to those rules of behavior not required by law but voluntarily self-imposed, which must be disclosed to act under these rules. In my opinion, it is a matter of consolidating or materializing the ethical decision-making process through reliable actions.

Therefore, self-regulatory mechanisms are the third pillar or cornerstone of the virtuous triangle to guarantee the right to privacy and PDP. Some self-regulatory mechanisms deserve special attention, such as certifi-

11 Regulation 2016/679 of the European Parliament and the Council of April 27, 2016. Available at https://www.boe.es/doue/2016/119/L00001-00088.pdf.

12 De Zan, Julio. "*Conceptos de 'ética' y moral*" (Concepts of ethics and principles), p. 22. Available at https://archivos.juridicas.unam.mx/www/bjv/libros/5/2228/4.pdf.

13 Navarro García, Fernando. *"El triunvirato entre* ética*, ley y compliance"* (Triumvirate among ethics, law, and compliance), European Journal compliance and news, p. 46. Available at http://www.aeaecompliance.com/images/documentos/revista5/j5navarro.pdf.

14 *Ibíd*.

cations, to keep a respectful approach to crucial rights and freedoms. For example, the deployment of information security management systems includes specifications for assets containing personal data, such as ISO 27000 international standard, specifically 27701, and the implementation of codes of ethics for each sector, implementation of internal policies, and even the adoption of measures excluded from the Law for the sake of proactive compliance.

As an example of the above, in Mexico, under public sector legislation, regulated entities require a PDPIA "*when trying to enforce or amend public policies, programs, systems or IT platforms, electronic applications, or any other technology involving intensive or relevant processing of personal data. Likewise, assess the actual impacts concerning specific processing of personal data to identify and mitigate potential risks related to the principles, duties, and rights of data holders and the responsibilities of those in charge, as provided in the applicable regulation*."[15]

On the other hand, legislation covering the private sector does not require an EIPD. Still, it is considered a practical recommendation, and it is up to the entity to decide whether to put it in place or not. In the latter case, we are under a self-regulated system already set and proposed in the Law.

03

STRENGTHENING OF INTERNATIONAL AND NATIONAL REGULATIONS UNDER A DEEP GLOBAL MARKETPLACE

The mismatch of domestic regulations is a significant challenge that started since the e-commerce boom. The *Global Privacy Assembly* ("GPA"),[16] in its Working Plan 2021-2023, set a priority strategy, which entails a global regulatory framework with high and clear standards consistent with PDP as digitalization moves at a swift pace.

The fact that rules have borders (unlike e-commerce or international data flow) causes disadvantages and legal uncertainty for personal data holders. They will rely on the practices of the company with whom they contracted goods or services and the legislation of the country where the company is based.

As the UK Information Commissioner, Elizabeth Denham, stated at the 43rd Global Privacy Assembly conference: "If, for example, a foreign company breaches its Law or of the country of the data holder and with whom it is doing business, or if there is a security breach, it would be highly complicated for regulatory agencies or PDP guarantors to work together due to issues of jurisdiction and legal systems."[17]

In the words of the former Commissioner, "*The result of all of the above is an international problem that may be costing trillions of dollars to worldwide economies.*" As she also points out, the meeting point of common standards and a better law structure can decrease the problem. However, we information commissioners cannot regulate, since we do not have legislative powers, although we can encourage and foster international discussion with legal bodies to reach consensus and improve our domestic regulations. PDPIA "

While there are no easy solutions, I think an approach to that meeting point lies in PDP and privacy principles. We are already working on the fundamental PDP principles to be accepted by the GPA State Membership. Still, the convergence process must speed up since we take a long time to respond, considering the transfer of personal data in the global data economy.

15 *Artículo 3, fracción XVI de la Ley General de PDP en Posesión de Sujetos Obligados*. (Article 3, section XVI – General Law of PDP owned by regulated entities).

16 *The GPI "…first named as the International Conference of Data Protection and Privacy Commissioners until the 41st Conference, has been the premier meeting place of the world's data protection and privacy regulators and enforcers. The Assembly has grown substantially, and its membership now extends across many parts of the world."* Available at: https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/ (viewed on March 15, 2022).

17 See https://globalprivacyassembly.org/solving-the-billion-dollar-question-how-do-we-build-on-the-foundations-of-convergence/ (viewed on March 14, 2022).

04

STRENGTHENING OF PUBLIC BODIES THAT GUARANTEE PDP AND PRIVACY, AND PROMOTING THE CREATION OF PUBLIC CYBERSECURITY AGENCIES

It is undeniable that organizations, by its nature, are looking to increase their power and control people's behaviors as much as possible. The State must prevent such situations to ensure the personal welfare of individuals and preserve the legal structure and public nature of authority. To this end, we need specialized bodies and institutions.

The agencies, institutions, or public bodies responsible for protecting personal data have the mandate of protecting and safeguarding this fundamental right. Caring for their autonomy and promoting its strengthening is essential for democratic systems. Watching people's data and personal lives means safeguarding their dignity and independence. As Philosophy & Ethics professor Carissa Véliz from Oxford University says: "Only to the extent that we take care of such autonomy is that they can make independent decisions and exercise complete freedom."[18] Thus, privacy is power. If people are empowered, they can make better decisions geared towards strengthening democratic systems and living in full where they can properly enforce their rights and freedom.

Part of the great challenge for data protection and privacy guarantor agencies is to raise awareness among the population, inform them, and promote their rights in this area to control their data (strengthening informational self-determination) and protect themselves against possible privacy vulnerabilities.

I also believe it is vital that States invest in cybersecurity and promote the creation of public cybersecurity bodies.

The protection of information assets, including personal data, is indispensable in our society because there are many risks in the online and offline environment; cyber-attacks are from day to day and increasingly sophisticated.

For years now, but to a greater extent due to the COVID-19 pandemic, societies have been steeped in the digital world and increasingly dependent on technology. Even when it comes to critical infrastructures, such as supply chains, transportation, and financial transactions, fundamental rights such as education and utility services, among others, currently operate through digital technologies. Therefore, we need an entity that ensures the privacy and security of personal data and our integrity and property.

We have seen alarming cases where malware exploits vulnerabilities in medical scanning equipment to step in and modify information and make cancerous nodules appear on an X-ray where there are none.[19] Or vice versa, a cyber-attack that almost contaminated a dam in the State of Florida in the USA.[20]

According to the Cybersecurity Report 2020 called Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean,[21] "the economic damage from cyber-attacks could exceed 1 percent of some countries' gross domestic product ("GDP"). In the case of attacks on critical infrastructure, this figure could reach up to 6 percent of GDP."

Since 2012, the United Nations Human Rights Council has acknowledged that human rights must be guaranteed online and offline.[22] It called upon all States to bridge the digital divide and increase the use of information and communications technology to encourage the full enjoyment

18 Véliz Carissa, *Privacidad es poder* ("Privacy is Power"), p. 89.

19 See "Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists," available at https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/ (viewed on March 14, 2022).

20 *Ibid.*

21 *Banco Interamericano de Desarrollo, Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf*. (Interamerican Development Bank, Report-2020- Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean), p. 10 (viewed on March 14, 2022).

22 "*Afirma que los mismos derechos que tienen fuera de línea las personas también deben protegerse en línea, en particular la libertad de expresión, lo que es aplicable independientemente de las fronteras y por conducto de cualquier medio de su propia elección, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos*;" p. 4. ("Article 19 of the International Covenant on Civil and Political Rights states that the same rights available off-line must be likewise true on-line, specifically relative to freedom of speech, which must be enforced regardless of the means the user chooses). Available at: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf (viewed on March 14, 2022).

of human rights for all by fostering an enabling, safe, and secure online environment conducive to the participation of all.

Therefore, I think it is essential to promote the creation of public cybersecurity agencies or institutions. We need specialized personnel to reinforce the lines of action already in different sectors. For example, in México, there are regulations relative to obligations in cybersecurity, especially in personal data security and other sectors such as telecommunication networks. Thus, we need an entity to lead the cross-cutting policies in this area, develop digital confidence among citizens and organizations, raise awareness and provide education on the subject matter to protect our fundamental rights in the digital arena.

> ***Since 2012, the United Nations Human Rights Council has acknowledged that human rights must be guaranteed online and offline***


DGA

"FIRST ACT" OF THE EUROPEAN DATA ECONOMY – THE DATA GOVERNANCE ACT

BY DR. PAUL VOIGT

& DANIEL TOLKS

Dr. Paul Voigt is Partner at Taylor Wessing in Berlin, Germany. Daniel Tolks is Attorney at Taylor Wessing in Berlin, Germany.

01 INTRODUCTION

In April 2022, the European Parliament will cast its vote on the Data Governance Act ("DGA"), which is the first measure in the course of the European Data Strategy. Correspondingly, high expectations are associated with this. The text of the first draft presented by the Commission in November 2020 was negotiated in detail in several trilogue discussions between the European Council, Parliament and Commission in October and November 2021 ("DGA-draft"). Thus, the final vote is only considered a formal step. The following article is therefore intended to provide a cursory overview of the main regulations as they currently stand, highlighting key

changes from the trilogue discussions and providing a preliminary assessment of the proposed measures.

02 OVERVIEW

A. General Categorization

The DGA-draft represents the first measure from the European Data Strategy published by the EU Commission in 2020. The latter aims to create European data spaces – i.e. an EU single market for data – in which both personal and non-personal data can be securely stored, processed, and used to create value. The DGA-draft sets a structural regulatory framework with regard to some actors considered crucial in this context. Despite the ambiguous title, it is a regulation that therefore does not require an implementation act by the member states. The regulation is to apply 15 months after its entry into force (Art. 35 DGA-draft).

B. Objectives and Scope of Regulation

The objective of the DGA-draft is to promote the availability of data by increasing trust in certain data-providing actors and strengthening data sharing mechanisms in the EU. For this purpose, the DGA-draft addresses four – in some cases very different – regulatory priorities (Art. 1(1) DGA-draft):

- Re-use of protected data held by public sector bodies (Chapter II),
- Data intermediation services (Chapter III),
- Data altruism (Chapter IV), and
- Creation of a European Data Innovation Board.

For these regulatory areas, the DGA-draft determines basic material as well as formal conditions and a corresponding supervisory framework.

C. Extensive Restrictions

Despite – or precisely because of – the broad range of topics addressed by the DGA-draft, there are extensive restrictions regarding the scope of application right at the beginning. Article 1(2) of the DGA-draft explicitly states that the DGA-draft is not intended to impose an obligation on public sector bodies to permit the re-use of data. Any rights of access to specific data sets or documents thus continue to be governed exclusively by national law.

The relation to other laws dealing with data processing is also explicitly clarified. According to Art. 1(2a) DGA-draft, Union and Member State data protection law, in particular the GDPR and the e-Privacy Directive, shall prevail. Equally, the powers and competences of the data protection supervisory authorities shall remain unaffected. Thus, to the extent that personal data is to be re-used under the DGA-draft, all of the requirements of the GDPR must additionally be observed, which is likely to raise a large number of detail questions in practice. Furthermore, the DGA-draft shall be without prejudice to competition law and the law of public security, defense, or national security pursuant to Art. 1(2b) and (2d) DGA-draft.

03 RE-USE OF PROTECTED DATA HELD BY PUBLIC AUTHORITIES

A. Background

Chapter II sets out the conditions for the re-use of data that is held by public sector bodies and protected for certain reasons. The background of the regulation is the idea that data generated or collected with the help of public funds should also benefit society (Rec. 5).

Chapter II can only be understood against the background of the OD-PSI Directive.[2] Since the scope of the OD-PSI Directive is limited only to "open data" that can be freely used by anyone, the DGA-draft now also regulates, in a complementary manner, the re-use of such data that is subject to the rights of others. Article 3(1) of the DGA-draft conclusively lists commercial secrecy (including business, professional and trade secrets), statistical secrecy, the protection of the intellectual property of third parties and the protection of personal data as such grounds of protection.

B. No Right to Data Access

It is important to emphasize that the DGA-draft does not create a right to re-use of these data (again stated in Art. 3(3) DGA-draft). Rather, it lays down basic conditions under which the re-use – which is presumed to be permitted – shall be structured. First of all, Art. 4 DGA-draft stipulates the fundamental prohibition of exclusive agreements in order to prevent any unfair competition. Exceptions may ex-

2 Directive 2003/98/EC on the re-use of public sector information.

ist if services are provided in the public interest that would not be possible without such exclusive agreement. It should be noted that the exclusivity period under Art. 4(5) and (7) DGA-draft was shortened considerably in the trilogue discussions: For new contracts it is now 12 months (previously three years) and for existing contracts 30 months (previously also three years).

C. Conditions for Continued Use

Art. 5 DGA-draft then lists, as the core of the chapter, various different conditions for re-use. Art. 5(2) DGA-draft stipulates that the conditions for re-use must be "non-discriminatory, transparent, proportionate and objectively justified." According to Art. 5(3) DGA-draft, the public sector bodies shall then ensure that the protective nature of the respective data is preserved. This can be achieved, for example, by anonymizing persona data, or by modifying or aggregating non-personal data like trade secrets or content protected by intellectual property rights. It may also be required that access to and re-use of the data must be made within a "secure processing environment," the technical integrity of which shall be verified by the public body. This can be done remotely or, if necessary, on premise. Access to the data shall also be made conditional on the adherence to a confidentiality obligation (Art. 5(5a) DGA-draft).

If re-use cannot be permitted and a legal basis for the (re-) processing of personal data is lacking, the public sector body should, according to Art. 5(6) DGA-draft, make best efforts to support in obtaining appropriate consents from the data subjects. Furthermore, the re-use of data is only permitted if intellectual property rights are respected, whereby public bodies cannot invoke the database producer right (Art. 5 (7) DGA-draft).

Although the conditions were specified in the course of the trilogue discussions, they still leave considerable room to the national public sector bodies to decide on the precise details. It is questionable how the public bodies will manage the balancing act between ensuring the protective nature of the data on the one hand and enabling re-use on the other.

D. Third-country Transfers

The provisions on the transfer of non-personal data to (non-EU) third countries have been aligned with the procedures of the GDPR. According to Art. 5(8a) DGA-draft, the intended third country transfer must first be notified to the public body. According to Art. 5(10) DGA-draft, the public sector body may only transfer the requested data to the re-user if the Commission has declared the recipient country's laws on the protection of intellectual property and trade secrets to be equivalent to EU standards (Art. 10b DGA-draft) or the re-user contractually undertakes to comply with the terms of the DGA-draft. In doing so, the public sector body shall support the re-user in implementing these obligations pursuant to Art. 5(10a) DGA-draft, for which standard contractual clauses may also be issued by the Commission.

This mechanism, already known from the GDPR, thus also applies to non-personal, sensitive data under the DGA-draft. In addition, the Commission may still adopt special conditions for the third country transfer of such categories of data that are classified as "highly sensitive" by separate EU legal act, for example in the area of public security or health (Art. 5(11) DGA-draft).

E. Procedure

According to Art. 6 DGA-draft, public sector bodies may charge proportionate and objectively justified fees for the re-use of data. According to Art. 8 DGA-draft, the competent Member State authorities shall establish a "single information point," which receives the requests for re-use of data and forwards them to the competent public sector body. On the initiative of the European Parliament, the trilogue discussions also included the possibility of establishing a simplified information channel for start-ups and small and medium-sized enterprises (SMEs), adapted to their specific needs, Art. 8(2b) DGA-draft. In this context, it is also important to note Art. 8a (1) DGA-draft, which stipulates that applications for the re-use of data must be regularly decided within two months; in extensive cases, the public sector body has a further 30 days.

The simplified application process and the short decision period are to be welcomed from the point of view of the re-users, since in this way innovative, data-based solutions can also be sought for current phenomena – e.g. regarding data from the COVID-19 pandemic. However, in view of the administrative burden required for this, it remains to be seen how this administrative simplification will play out in practice.

04
DATA INTERMEDIATION SERVICES

A. Background

Chapter III establishes a notification and supervision framework for so-called data intermediation services. According to the definition in Art. 2 (2a) DGA-draft, these are services which aim to establish commercial relationships for the purpose of data sharing between an undetermined number of

data subjects and data holders, on the one hand, and data users on the other hand, through technical, legal, or other means.

The background to the regulation is the expectation that independent data intermediaries will play a key role in the data economy by contributing to the efficient pooling of data sets and facilitating the exchange of data, especially between companies, while also providing SMEs and start-ups with non-discriminatory access to the data economy. This is related to the envisaged creation of common European data spaces, i.e. sector-specific or cross-sector interoperable frameworks with common standards and procedures for data sharing, including for the development of new products and services, scientific research, or civil society initiatives (Rec. 22).

B. Concept of Data Intermediary according to the DGA-Draft Definition.

With the term "data intermediary," the DGA-draft thus aims at a new form of data sharing associated with thoroughly ambitious visions of the future. While the Commission proposal still referred to "data sharing services" throughout, the negotiated version of the DGA-draft now explicitly introduces the concept of data intermediary. Extensive additions have also been made – particularly in Rec. 22 ff. – to clarify the concept of data intermediary.

However, according to the definition in Art. 2 (2a) DGA-draft, services that aggregate, enrich, or transform data in order to add significant value to it and grant licenses for the use of the resulting data without establishing a direct relationship between data owners and data users are not to be considered data intermediation services. Also excluded are services aimed at mediating copyrighted content and services used by a data owner or by multiple legal entities in a closed group (including supplier or customer relationships) to enable internal data use (especially in the context of the Internet of Things).

"With the term "data intermediary," the DGA-draft thus aims at a new form of data sharing associated with thoroughly ambitious visions of the future

C. Further Specifications in the Recitals

Rec. 22a provides some practical examples of services that should or should not be considered as data intermediation services. No data intermediation services are the provision of cloud storage, analytics or file sharing software, web browsers or browser plug-ins, and email services, as long as such services only provide technical tools to share data with others but are not used to establish a commercial relationship between data holders and data users. In contrast, examples of data intermediation services include data marketplaces where companies can make data available to third parties, data sharing organizers in European data rooms that are open to all interested parties, and data pools that are set up by several legal or natural persons in such a way that the possibility of using the pool results from the own contribution to it.

Although the term "data intermediary" has been somewhat clarified by these additions, numerous difficulties of delimitation are likely to continue to arise in practice. For example, the European map service provider "Here Technologies" raised the concern that data sets offered to businesses - i.e. navigation services and high-resolution maps - could fall under the DGA-draft, which could require the separation of domains and the interposition of a data intermediary. Although the aforementioned case is likely to correspond to one of the exceptions in Art. 2(2a) DGA-draft, as the data are processed in a value-added manner, the example illustrates the uncertainty in applying the vague concept in practice.

D. Registration Requirement and (Extended) List of Obligations

Art. 9 DGA-draft establishes a control mechanism for data intermediation services, which can be summarized as a notification requirement and ex-post supervision. Art. 10 DGA-draft provides for a formal notification procedure and Art. 11 DGA-draft for material requirements, including the preservation of the purpose of the data, the process and price design, the format and transformation of the data, measures for fraud prevention, insolvency protection, technical, legal, and organizational measures to prevent unlawful transfers, and security measures for storage.

The conditions have been extended in the course of the trilogue discussions. For example, Art. 11(4a) DGA-draft now stipulates that data intermediaries may, with the consent of data holders, offer additional services that serve to facilitate data exchange, such as temporary storage, curation, conversion, anonymization and pseudonymization. Although this makes sense from a practical point of view, it will probably raise numerous detail questions, particularly with regard to the definition of data intermediary in Article 2 (2a) (a) DGA-draft, according to which the aggregation, enrichment or transformation of data is to be regarded as an exclusion criterion. Furthermore, the interoperability with other data intermediaries shall be ensured through the use of general standards (Art. 11 (6a) DGA-draft) and a log of the intermediation services is to be prepared (Art. 11 (11a) DGA-draft).

E. Supervisory Framework

Data intermediation services do not require regulatory approval. Nevertheless, to the extent that a violation of Art. 10 or 11 DGA-draft has been established, the competent authority may order the termination of the service or impose "dissuasive fines" (Art. 13 (4) DGA-draft). To ensure law enforcement, providers must be established in the EU or designate a legal representative in the EU (Art. 10(3) DGA-draft). In addition, private enforcement by data owners, users or competitors may also be considered.

F. Assessment

The strict obligations for data intermediaries and the notification and supervision framework leaves a mixed impression. On the one hand, one could assume that they create trust in data intermediaries and prevent misuse of the data trustee model. On the other hand, imposing additional stricter requirements than already exist in data privacy and IT security law may potentially inhibit innovation. Indeed, one can doubt whether the regulations on data intermediaries will be understood in practice as an incentive to share data. Even if the regulatory approach may counteract any misuse of the data trustee model, the question arises as to whether this could not have been better achieved with a voluntary certification system that is linked, for example, to certain privileges under data protection law. It therefore remains to be seen whether the DGA-draft will boost the market for data intermediaries, in view of rising compliance costs and limited scope for new business models.

05
DATA ALTRUISM

A. Concept

As another major topic, Chapter IV regulates so-called data altruism. Data altruism, according to the definition in Art. 2(10) DGA-draft, is the voluntary sharing of data on the basis of data subjects' consent to the processing of personal data relating to them or the permission of other data controllers to use their non-personal data free of charge for purposes of general interest. The DGA-draft cites as examples of such purposes: health care, combating climate change, improving mobility, facilitating the production of official statistics, improving public services, shaping public policy, or scientific research purposes in the general interest.

B. Recognition as a Data Altruistic Organization

Pursuant to Art. 16 et seq. legal entities that strive to promote the aforementioned objectives may register as "data altruistic organizations recognized in the Union." The prerequisite is that these organizations operate on a non-profit basis and are legally independent, and also fulfill extensive transparency and record-keeping obligations, for example with regard to data processing, purpose tracking and sources of income. Rec. 36 lists further requirements, e.g. a secure processing environment and the establishment of ethics councils, which, however, have not found their way into the enacting terms of the DGA-draft and whose enforceability therefore appears to be questionable.

According to Article 15 of the DGA-draft, registration allows the organization to use the designation "data altruistic organizations recognized in the Union" (including a corresponding logo), which essentially offers the advantage of a *de facto* leap of faith . In addition, registered data altruistic organizations are exempt from the rules on data intermediaries (Art. 14 DGA-draft). According to Art. 15 DGA-draft, the competent authority keeps a register of recognized data altruistic organizations and can remove the respective organization from the register in case of violations (Art. 21). There are no more severe sanction options, which is to be understood against the background that data altruistic organizations may also operate without registration, but then may have to comply with the conditions for data intermediaries.

C. Member State Funding and Data Altruistic Rulebook

Added in the trilogue discussions is Art. 14a DGA-draft, according to which member states can also promote data altruism by creating a framework in which data subjects can altruistically share such data that is stored with public service providers; in Germany, this is already the case with the electronic patient file (Section 363 (1) SGB V). Furthermore, Art. 19a DGA-draft was introduced, which requires the Commission to issue a "rulebook" setting out further requirements. These relate to information requirements for the consent of data subjects or the permission of other data holders, appropriate security requirements to ensure an adequate level of security for data storage and processing, multidisciplinary "communication roadmaps" to raise awareness among the relevant stakeholders, and recommendations on interoperability standards. According to Art. 19a (2) DGA-draft, the "Rulebook" is to be drafted in cooperation with data altruistic organizations, but at the same time compliance with it is to be a prerequisite for recognition as a data altruistic organization according to Art. 16 DGA-draft (after an 18-month implementation period). It is highly doubtful whether such additional "rulebook" is necessary – at least to the extent that it not only specifies existing obligations (such as information obligations under the GDPR), but also creates entirely new ones.

D. European Consent Form

In order to facilitate the consent of data subjects, which is often required for altruistic data collection, Art. 22(1) DGA-draft provides that the Commission – in consultation with the European Data Protection Board as well as the European Data Innovation Board to be created (on the latter see below) – shall adopt implementing acts establishing a European consent form. In terms of content, Article 22(2) DGA-draft specifies that the consent form should follow a modular approach so that it can be adapted to specific sectors and for different purposes. According to Art 22 (4) DGA-draft, the form shall be provided in a form in which it can be printed on paper and is easily understandable, as well as in electronic, machine-readable form. Conversely, it follows from Art 22(3) DGA-draft that the form not only applies to consents under the GDPR but can also be used for permissions regarding non-personal data.

E. Assessment

Thus, it is clarified that consent is also required for data use for altruistic purposes, which therefore must meet all requirements of the GDPR (including purpose limitation and the possibility of withdrawal at any time). This will put significant burden on organizations trying to pursue altruistic objectives. At least, the consent form offers the advantage of obtaining consent in all member states in a uniform format, which should serve legal certainty. The question of the extent to which the form published by the Commission can also be used as a model for consent declarations outside the scope of the DGA-draft is also likely to be interesting. Rec. 39 p. 4 DGA-draft provides for the possibility of sector-specific adjustments of the consent form, which might indicate its use in different fields of application.

06
EUROPEAN DATA INNOVATION BOARD AND FURTHER ISSUES

A. Creation of a European Data Innovation Board

Art. 26 DGA-draft provides for the establishment of a "European Data Innovation Board" in the form of an expert group composed of, among others, representatives of the Member State authorities, the European Data Protection Board and other European institutions and expert bodies. The European Data Innovation Board has the tasks set out in detail in Art. 27 DGA-draft. These include advising and assisting the Commission in developing a consistent practice with regard to the topics of the DGA-draft and developing guidelines (in particular with regard to the creation of common European data spaces). Particularly because many of the provisions of the DGA-draft are rather general, the Innovation Board is to be expected great importance in interpreting the DGA.

B. Third-Country Access and Transfers

In the final provisions in Chapter VIII, the DGA-draft contains general provisions relating to the protection of non-personal data in the context of official or judicial third-country access and transfers. According to these, all addressees of the DGA-draft must take appropriate technical, legal, and organizational measures to prevent the transfer of or access to non-personal data stored in the Union if such transfer or access is contrary to Union law or the law of the Member State concerned (Article 30(1) DGA-draft). Corresponding transfers are to be permitted only if they can be based on an international agreement in force, such as a mutual legal assistance treaty, (Art. 30(2)), or if certain rule of law criteria listed in Art. 30(3) DGA-draft are met in the third country concerned.

07
CONCLUSION

The DGA-draft is intended to represent a first approach to the creation of an EU single market for data. However, the extent to which this will actually advance the European data economy remains to be seen – especially after the trilogue discussions. In view of the numerous (additional) obligations that the DGA-draft imposes on public bodies, data intermediaries and data altruistic organizations that are basically willing to share, one may well raise the question as to whether this will not rather have the opposite effect. This applies in particular to the notorious exclusion of data protection law. The existing data protection rules under the GDPR create imponderables in many respects. This concerns, for example, the relevant legal basis (legally disputed data contract or consent with the risk of withdrawal at any time), the role of the actors under data protection law (legal substitutes outside Art. 80 GDPR) or structural contradictions (data minimization vs. interest in extensive data pools). There is no shortage of proposed solutions for this. These range from facilitating consent (e.g. reducing formal requirements, enabling "broad consent" and waiving withdrawal to a certain extent), creating area-specific exceptions under Art. 2(2) or 85 of the

GDPR, or introducing voluntary certifications leading to more extensive processing possibilities under data protection law. However, these proposals have not been considered for the DGA-draft. Therefore, legal uncertainties remain that slow down the envisaged creation of European data spaces.

> *The DGA-draft is intended to represent a first approach to the creation of an EU single market for data*


16
Bundeskartellamt

FACEBOOK v. BUNDESKARTELLAMT – MAY EUROPEAN COMPETITION AGENCIES APPLY THE GDPR?

BY
ANNE C. WITT

Professor of Law, EDHEC Business School, Augmented Law Institute. Email: anne-christine.witt@edhec.edu.

01 INTRODUCTION

Privacy and competition law have long been considered separate areas of law, guided by different objectives and enforced by different agencies. Competition law aims to protect competition, and privacy law aims to protect the personal information of individuals. In the age of data-driven business models, however, where consumers receive free services in exchange for their data, the dividing lines have become blurred. If a digital platform restricts competition by foreclosing competitors or acquiring a competitive threat, and is consequently able to degrade its privacy standards, is this a relevant form of harm within the

meaning of competition law? If a dominant platform uses its near monopoly position to impose supra-competitive data-collection terms on users, should this be considered an abuse of dominance? The German Bundeskartellamt made the headlines in 2019, when it answered the latter question in the affirmative, and prohibited Facebook's data collection terms as incompatible with German competition law.

The case persuaded the German legislator to amend the German competition act, and set in motion a long and complex judicial review process. It has now reached the European Court of Justice, which has been asked to clarify whether national competition agencies may apply the GDPR in competition law cases.[2] This short contribution critically discusses the request for a preliminary ruling in *Facebook v. Bundeskartellamt*, and argues that national competition agencies should be permitted to interpret national competition rules in line with the GDPR.

02

THE UNDERLYING FACTS, ACCUSATIONS AND PROCEDURE

The facts underlying the original case are well known. Because of its innovative – and highly controversial – theory of harm, the German competition agency's prohibition from February 2019 attracted a great deal of attention in the international press[3] and scholarship.[4] In all brevity, the reference that is currently pending before the European Court of Justice in *Facebook Inc. and Others v. Bundeskartellamt,* relates to the decision of the German competition agency ("Bundeskartellamt") of February 2019 to outlaw Facebook's data collection policy under German competition law.[5] In essence, the Bundeskartellamt held that Facebook's policy of collecting and combining personal user data from different sources (i.e. the social network itself, any Facebook-owned business, and any of the millions of third-party businesses worldwide that have incorporated Facebook business tools into their websites) amounted to an exploitative abuse of Facebook's market power on the German market for personal social networking services.

The agency argued that Facebook had used its position of dominance to force excessive data collection terms upon consumers, which the latter had no choice but to accept for want of a reasonable alternative: if consumers wished to use a social network of a workable scale, they had to agree to Facebook's data collection terms. According to the Bundeskartellamt, this harmed consumers because it violated their constitutional right to privacy. The agency inferred the infringement of this constitutional right from the fact that, in its view, Facebook's conduct was incompatible with the "principles"[6] guiding the European Union's General Data Protection Regulation ("GDPR").[7] To this end, the Bundeskartellamt carried out a 100-page assessment of Facebook's data collection policy under the "principles" of the GDPR. In substance, this amounted to an in-depth analysis of whether Facebook could invoke any of the legal justifications stipulated in Article 6 and 9 GDPR.

Throughout the process, the Bundeskartellamt liaised and consulted with the German data protection agency on the interpretation of the GDPR. Having reached the conclusion that Facebook's conduct was incompatible with the prin-

2 Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on April 22, 2021 in Case C-252/21 *Facebook Inc. and Others v. Bundeskartellamt.*

3 E.g. Sam Schechner and Sara Germano, "Facebook Told to Stop Tracking German Users' Online Life Without Consent," The Wall Street Journal (February 7, 2019); Olaf Storbeck, Madhumita Murgia and Rochelle Toplensky, "Germany blocks Facebook from pooling user data without consent," Financial Times (February 7, 2019); Natasha Singer, "Germany Restricts Facebook's Data Gathering" The New York Times (February 7, 2019); Cécile Boutelet, "L'Allemagne dénonce la position dominante de Facebook sur la collecte de données personnelles," Le Monde (February 7, 2019.

4 See e.g. Anne Witt, "Excessive Data Collection as a Form of Anti-Competitive Conduct – the German Facebook Case," (2021) 66(2) *Antitrust Bulletin* 276–307; Viktoria Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data," (2020) 57 Common Market Law Review 161–189; Marco Botta and Klaus Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey', (2019) 64(3) Antitrust Bulletin 428–446.

5 Bundeskartellamt, decision no B6-22/16 of February 6, 2019. Because of the significance of the decision, the Bundeskartellamt provided an English translation of the decision, available at http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-%2022-16.pdf?__blob=publicationFile&v=4.

6 "Wertungen" in the original.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L119/1.

ciples of the GDPR, and having concluded that Facebook's position of dominance was causal for this harm, the agency found that Facebook had committed an abuse of dominance within the meaning of sec. 19(1) GWB.[8] It ordered Facebook to amend its data collection policy, but did not impose a fine.

> ***Throughout the process, the Bundeskartellamt liaised and consulted with the German data protection agency on the interpretation of the GDPR***

Facebook appealed, and applied for interim relief. The Düsseldorf Higher Regional Court was convinced by Facebook's arguments, and, in an unusual move, ordered suspensive effect of the appeal. In a strongly worded interim order,[9] it stated that it was obvious that the prohibition could not be upheld in the main proceedings because of serious legal errors. Among others, the Düsseldorf Higher Regional Court, while also disputing the very concept of harm used by the agency, fundamentally disagreed with the Bundeskartellamt's assessment that Facebook users had not freely consented to the data collection within the meaning of Articles 6(1)(a) and 4(11) GDPR because of a lack of choice. It took the view that users had had a very clear choice: they could opt to accept Facebook's contractual conditions and use the network, or they could follow the example of 55 million German residents and choose not to use Facebook. Facebook had not coerced or swindled its users. It had laid out its contractual terms in diverse policy documents that consumers had the possibility of accessing online. If users were too lazy to read these documents in detail, but simply ticked a box accepting the terms and conditions, this did not call into question the freedom of their choice.

The Bundeskartellamt appealed to the German Federal Court of Justice, Germany's highest court of ordinary jurisdiction, which sided with the agency and struck down the Düsseldorf Higher Regional Court's interim order.[10] The Federal Court of Justice did not consider the decision sufficiently flawed to justify interim relief. On the contrary. While the court formally merely reviewed whether interim relief was called for, it made clear between the lines that it had little doubt that Facebook had committed an exploitative abuse. It did not call into question the Bundeskartellamt's privacy-based concept of harm. It confirmed that the right to data protection was covered by the constitutional right to privacy and stressed the particular importance of protecting data generated on social networks against exploitation by network operators because of the political and economic significance of online communications and the sensitivity and depth of such data. The court also confirmed that public bodies were required to consider this constitutional right when interpreting open-worded legal rules such as the prohibition of abuse of dominance, even if the rule in question regulated a relationship between private actors. While the Federal Court of Justice thus ruled that sec. 19 GWB had to be interpreted in light of the German constitutional right to privacy, and not the GDPR, it also clarified that the Bundeskartellamt was entitled to take into account the principles and values underlying the GDPR in this process.[11]

The Federal Court of Justice further strongly disagreed with the Düsseldorf Higher Regional Court's view that users had been able to make a free and autonomous decision whether to consent to the data collection. It criticized that, by focusing entirely on the lack of coercion and the freedom not to use Facebook, the lower court had failed to consider that for many users, communication via Facebook had become an indispensable part of their social interactions and a means of participating in society. The fact that 80 percent of users questioned had admitted to not having read Facebook's terms and conditions was evidence of information asymmetry and rational apathy of users who thought they had no leverage, rather than indifference about the use of their personal data. Facebook had therefore deprived consumers of an important choice that would have existed in a competitive market, i.e. the choice between the use of (1) a highly personalized social network service for which consumers agreed to extensive data collection from Facebook and "off Facebook," and (2) a less personalized service that relied only on the data users chose to disclose on Facebook. The Federal Court of Justice, failing to see any serious errors of law, therefore annulled the lower court's interim order granting suspensive effect of the appeal.

8 Gesetz gegen Wettbewerbsbeschränkungen (GWB). Available at https://www.gesetze-im-internet.de/englisch_gwb/.

9 OLG Düsseldorf, Order of 9 January 2015, Az. VI Kart 1/14 (V), available at https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2019/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf.

10 Bundesgerichtshof, order of June 23, 2020 in Case KVR 69/19 – *Facebook*.

11 Bundesgerichtshof, order of June 23, 2020 in Case KVR 69/19 – *Facebook*, paras 102-110.

03
THE CONTROVERSY

The Bundeskartellamt's Facebook decision raises many interesting issues of competition law relating to causality, market definition and market power analysis in markets for free services. In addition, however, it brought to the fore a much more fundamental issue. May competition agencies consider the impact on privacy when assessing the anticompetitive conduct of businesses? Should they evem do so? These are highly controversial questions, which are closely linked to an even more hotly contested issue: what is the legal objective of competition law? To what end do we protect competition in the market? This last question is as old as the law itself, and yet, has never been answered to the satisfaction of all.[12]

> ***The Federal Court of Justice further strongly disagreed with the Düsseldorf Higher Regional Court's view that users had been able to make a free and autonomous decision whether to consent to the data collection***

Several possibilities come to mind. One may take the view that the law should protect competition as such because of the many, often unquantifiable, advantages competitive markets tend to generate for society. These benefits include, but are not limited to, economic efficiency, economic freedom, freedom of opportunity, fairness, democracy and social welfare. Alternatively, one could take a narrower view and focus on a specific outcome. U.S. courts adopted such a narrow approach in the late 1970s, when the U.S. Supreme Court was convinced that the ultimate purpose of U.S. antitrust law should be to maximize consumer welfare, and that distortions of competition should only be sanctioned if they reduced such welfare.[13] The European Commission followed suit in the early 2000s, and also adopted consumer welfare as the ultimate aim of EU competition law.[14] While both the U.S. antitrust authorities and the European Commission define consumer welfare in terms of low prices, high output, high quality and high levels of innovation,[15] U.S. courts, in particular, have tended to focus primarily on prices and output in practice, as these are easier to quantify than reductions in quality or innovation.[16] This makes for a very narrow concept of harm indeed.

The right to privacy and data protection do not fall within the scope of this purely economic concept of consumer welfare. Unsurprisingly, therefore, the European Commission has taken the position in recent years that data protection and competition law are two distinct spheres of regulation, which should be kept separate. Since the advent of data-driven business models, it has had multiple opportunities to review business conduct that might affect user privacy under the competition rules. However, it did not consider the impact on privacy a relevant factor in any of these transactions. Instead, it focused exclusively on the conduct's impact on competition in terms of market shares, market concentration, barriers to entry and foreclosure effects. In its decision clearing Facebook's acquisition of WhatsApp, the Commission even explicitly stated that any privacy-related concerns arising from the combination of personal data as a result of the merger did not fall within the scope of EU competition law but that of EU data protection regulation.[17]

The U.S. antitrust authorities have taken a similar approach in their investigations of data-heavy transactions. In its assessment of the *Google/DoubleClick* acquisition from 2007, for example, the majority of the FTC clarified that privacy

12 For a brief account, see Anne Witt, 'Technocrats, Populists, Hipsters, and Romantics – Who Else is Lurking in The Corners of The Bar?" CPI Antitrust Chronicle (Nov. 2019).

13 E.g. *Reiter v. Sonotone Corp.*, 442 U.S. 330, 343 (1979).

14 See e.g. European Commission's Guidelines on the application of Article 81(3) of the Treaty of April 27, 2004, OJ [2004] C101/97, para 8.

15 European Commission, Guidelines on the application of Article 81(3), paras 17–25, or European Commission, horizontal merger guidelines, [2004] OJ C31/5, para 22; FTC and U.S. Department of Justice, Antitrust Guidelines for Collaborations Among Competitors (April 2000), p.4.

16 Marshall Steinbaum & Maurice E. Stucke, "The Effective Competition Standard: A New Standard for Antitrust," (2020) 85 Chicago University Law Review 595.

17 European Commission, decision of October 3, 2014 (Case COMP/M.7217 – *Facebook/WhatsApp*), recital 164.

concerns arising from the acquisition of user data were a matter for consumer protection and not antitrust law.[18] However, in the FTC's current case against Facebook, alleging a violation of section 2 of the Sherman Act by means of strategic acquisitions of competitive threats, the FTC explicitly included and even heavily emphasized the degradation of privacy protection by Facebook, once the market had tipped in its favor, as evidence of consumer harm in the form of reduced service quality.[19]

> ***The right to privacy and data protection do not fall within the scope of this purely economic concept of consumer welfare***

In sum, there is a fair amount of disagreement and even uncertainty among enforcement agencies on whether to incorporate the impact on privacy into competition law assessments if this harm was caused by a restriction of competition. The German legislator, incidentally, sided with the Bundeskartellamt, and explicitly clarified in a recent amendment[20] of the Germany competition statute that relevant harm within the meaning of the act is not limited to measurable monetary losses, but can also consist in the transfer of personal data.[21] Parliament thereby rejected the purely economic interpretation embraced by the Düsseldorf Higher Regional Court, currently also guiding the European Commission's interpretation of EU competition law.

The disagreement at the enforcement level is mirrored in the academic world. While there are commentators advocating a clear separation of privacy and competition law,[22] others are highly critical of this trend. The latter propose a number of ways in which privacy could be incorporated into competition law assessments. Many think it is wisest to frame privacy in terms of consumer welfare, which would facilitate its integration into the current economic consumer welfare standard. Among this group, there are proposals to look at data protection as a factor of service quality,[23] and suggestions to consider personal data the price that consumers pay for a service.[24] Others, finally, advocate abandoning the consumer welfare standard entirely, and to focus on protecting "effective competition,"[25] the "process of competition,"[26] "competitive market structures,"[27] or "consumer choice."[28]

18 FTC, 'Statement of the Federal Trade Commission Concerning Google/DoubleClick' of December 20, 2007, F.T.C. File No. 071-0170. Commissioner Pamela Jones Harbour issued a Dissenting Statement on this point (Dissenting Statement of Commissioner Pamela Jones Harbour Concerning Google/DoubleClick of December 20, 2007).

19 *FTC v. Facebook*, Case 1:20-cv-03590-JEB (Substitute Amended Complaint of September 8, 2021), para 222. Available at http://www.ftc.gov/system/files/documents/cases/2021-09-08_redacted_substitute_amended_complaint_ecf_no._82.pdf.

20 Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digital Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB-Digitalisierungsgesetz), BGBl 2021 I S. 2.

21 See e.g. the explanatory memoranda accompanying the legislative proposal: Bundesministerium für Wirtschaft und Energie, Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz), p. 72.

22 Justus Haucap, "Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of The German Facebook Decision," *CPI Antitrust Chronicle*, February 2019, 1 (this commentator advised Facebook in the proceedings before the FCO); Giuseppe Colangelo and Mariateresa Maggiolino, "Data Protection in Attention Markets: Protecting Privacy through Competition?" (2017) 8(6) *Journal of European Competition Law & Practice* 363; Maureen Ohlhausen and Alexander Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy', (2015) 80 *Antitrust Law Journal* 121; James Cooper, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity' (2013) *George Mason University Law and Economics Research Paper Series* 13-39.

23 Maurice Stucke, "Should we be concerned about data-opolies?" (2018) 2 *Georgetown Law Technology Review* 275.

24 Viktoria Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data" (2020) 57 *Common Market Law Review* 161.

25 Marshall Steinbaum & Maurice E. Stucke, 'The Effective Competition Standard: A New Standard for Antitrust', (2020) 85 *Chicago University Law Review* 595.

26 Warren Grimes, 'Breaking Out of Consumer Welfare Jail: Addressing the Supreme Court's Failure to Protect the Competitive Process', (2020) 15 *Rutgers Business Law Review* 49; Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*, Columbia Global Reports (2018).

27 Lina M. Khan, "Amazon's Antitrust Paradox," (2017) 126 *Yale Law Journal* 710.

28 Robert H. Lande, "The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern," 714 FTC:WATCH 9, February 25, 2008; Neil W. Averitt and Robert H. Lande, "Using the Consumer Choice Approach to Antitrust Law" (2007) 74 *Antitrust Law Journal* 175.

To say that the issue is controversial is probably understating the matter.

04 THE REFERENCE

The European Court of Justice has now been afforded the opportunity to rule on the issue. After the Federal Court of Justice struck down the Düsseldorf Higher Regional Court's interim order in June 2020, confirming the Bundeskartellamt's view that excessive data collection could theoretically constitute an abuse of dominance under German competition law, the main proceedings continued before the lower instance court. While it was for the Düsseldorf Higher Regional Court to decide the merits of the appeal, it was bound to follow the Federal Court of Justice's legal interpretation of the German competition rules. In particular it had to accept that, even in the absence of economic harm, excessive data collection could be abusive on the part of a dominant undertaking, at least under German competition law.

In April 2021, the Düsseldorf Court decided to stay the proceedings and make a reference for a preliminary ruling to the European Court of Justice.[29] In its request, it asked the European Court of Justice to provide guidance on the interpretation of the GDPR. All in all, it asked seven complex questions, many of which contained several subquestions.

> ***In April 2021, the Düsseldorf Court decided to stay the proceedings and make a reference for a preliminary ruling to the European Court of Justice***

Primarily, the Düsseldorf Higher Regional Court is seeking to establish whether a competition agency may apply the GDPR in the context of competition law assessments. In essence, it is asking the Court of Justice to rule on whether it is compatible with the enforcement system of the GDPR for a national competition agency, rather than a data protection agency, to establish an infringement of the GDPR for the purposes of proving a competition law infringement under national law, and to order the undertaking to end that breach. In addition, and depending on whether the Court of Justice considers that national competition agencies are indeed competent to apply the GDPR, the Düsseldorf court further asked the Court of Justice to clarify the meaning of several justifications available under the GDPR. In particular, it asked whether it was at all possible for a user to give "effective and free consent" to a dominant undertaking such as Facebook. It further requested that the Court interpret the concepts of "necessity for the performance of a contract" and the "pursuit of legitimate interests," and provide guidance on whether a user makes personal data public within the meaning of Article 9(2)(e) of the GDPR if he or she "likes" or "shares" certain posts on websites and apps.

05 ANALYSIS

What to expect from the preliminary ruling? The Court of Justice has been afforded the opportunity to provide important and much-needed guidance on several key concepts of the GDPR. However, according to the referring court's application, these questions are only to be answered if the European Court of Justice considers that a national competition agency may assess business conduct under the GDPR for the purposes of establishing a competition law infringement.

This is a complex issue. The Düsseldorf Higher Regional Court's questions on this matter are specific and narrow in scope. They are formally limited to issues of competence. The referring court did not ask the Court of Justice to rule on the objectives of EU competition law, or whether a negative impact on user privacy is a relevant form of harm under the EU competition rules. This is because the Bundeskartellamt did not apply Article 102 TFEU in addition to the German abuse of dominance rules, although, arguably, it should have.[30] Instead, the Düsseldorf Court therefore questioned the competence of the Bundeskartellamt to find that an undertaking had breached the GDPR, and to issue an order to end that breach. The GDPR, in Articles 51 et seq., establishes a rudimentary enforcement system through national supervisory authorities specifically tasked by each Member States with the enforcement

29 Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on April 22, 2021 in Case C-252/21 *Facebook Inc. and Others v. Bundeskartellamt.*

30 See e.g. Wouter Wils, "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt," 2019(3) Concurrences 58.

of the GDPR. The Bundeskartellamt is no such supervisory authority.

The key danger of a competition agency applying the GDPR is that of conflicting decisions and inconsistent interpretation. The competition agency may well reach a different decision than the supervisory agency of its State would have done. A second danger, if a competition agency assesses business conduct under the GDPR, is that it might undermine the GDPR's system of allocating competences between national supervisory agencies. According to Article 56(1) GDPR, it is the supervisory authority of the main establishment of the investigated company that shall be competent to act as lead supervisory authority for cross-border processing carried out by that company. In this specific case, the lead authority would be the supervisory authority of Ireland, where Facebook is established, and not Germany.

However, it is not clear that the Bundeskartellamt really established that Facebook had infringed the GDPR or that it had issued an order to end such a breach. The Bundeskartellamt was careful to stress throughout the decision that it was merely assessing the compatibility of Facebook's conduct with the "principles" underlying the GDPR, rather than the GDPR itself, in order to support its view that Facebook's data collection was excessive within the meaning of German competition law. It also did not formally establish an infringement of the GDPR. It established an abuse of dominance. Insofar, one could legitimately argue that the Bundeskartellamt did not directly enforce the GDPR, and therefore did not overstep its competences. Instead, it interpreted national (constitutional) law in light of the GDPR in an investigation under German competition law. Member States have a general obligation to interpret national law in line with EU law pursuant to Article 4(3) TEU. Also, if one required national public bodies to refrain from interpreting national law in line with the GDPR unless the competent supervisory agency had already pronounced itself on the case, this would significantly undermine the effectiveness of the GDPR.

The Court of Justice may well limit itself to answering the formal question of competence. It might, however, also take the reference as an opportunity to make a more sweeping pronouncement on the relationship between data protection and competition law, for example by indicating whether it considers a degradation of privacy a relevant form of harm if it is caused by the absence of competition or a distortion of competition. This is a highly contested issue, and one of great practical relevance. As national competition agencies are also competent to enforce Article 102 TFEU alongside the Commission, a clear statement on whether privacy is a relevant form of harm under EU competition law would contribute to the uniform interpretation of EU law at the national level.

Unlike the European Commission, the Court of Justice has never formally embraced economic consumer welfare as the exclusive legal objective of EU competition law. Its standard definition is that the function of these rules is to prevent competition from being distorted "to the detriment of the public interest, individual undertakings and consumers, thereby ensuring the well-being of the European Union."[31] This is a wider concept than the European Commission's view that the EU competition rules' objective is to protect competition to prevent business conduct that would deprive consumers of low prices, high quality products, a wide selection of goods and services, and innovation.[32] The Court's wider definition could theoretically accommodate a non-economic concept of harm, especially as the Court considers fundamental rights, such as the general right to privacy, now also enshrined in Art. 8 of the Charter of Fundamental Rights of the European Union, an integral part of the general principles of law the observance of which it ensures. It has repeatedly interpreted other areas of commercial law, such as the free movement rules, in light of EU fundamental rights. For example, it has held that fundamental rights, such as the freedom of expression, assembly, or the principle of human dignity, can act as limitations on the free movement of goods or services even if these aims are not explicitly listed in the relevant Treaty exemption.[33] In view of this case law, one could therefore argue that the right to privacy should be taken into account when assessing whether a restriction (or conduct in the absence) of competition led to a relevant form of harm.

> ***Unlike the European Commission, the Court of Justice has never formally embraced economic consumer welfare as the exclusive legal objective of EU competition law***

Moreover, is it really sensible to segregate privacy and competition law in the age of the digital economy? Where undertakings use data-based business models, the tasks

31 Case T-399/16 *CK Telecoms UK Investments Ltd v. European Commission*, ECLI:EU:T:2020:217, para 93 C-52/09 *TeliaSonera Sverige*, EU:C:2011:83, paras 20 to 22.

32 E.g. European Commission, Horizontal Merger Guidelines, [2004] OJ C31/5, para 8.

33 Cases C-36/02 *Omega* ECLI:EU:C:2004:614, para. 35; C-112/00 *Schmidberger* ECLI:EU:C:2003:333, para. 74; Case C-260/89 ERT ECLI:EU:C:1991:254, para 45.

of protecting users' privacy against the misuse of their data, and safeguarding competition against the abusive use of this data, are intrinsically linked. Regulating such business models in a judicious manner requires an interdisciplinary approach with input not only from competition lawyers and economists, but from privacy experts, IT technicians and psychologists. It also requires an interinstitutional approach, in which the different enforcement authorities liaise and advise each other on their respective areas of expertise. Attempting to solve privacy and competition issues in airtight institutional silos without regard to the conduct's impact on values that fall within the primary responsibility of another institution is going to lead to suboptimal, because unbalanced, results for society.

> ***Moreover, is it really sensible to segregate privacy and competition law in the age of the digital economy?***

Privacy and competition issues are inextricably connected in the case of data-driven business models. Not only can the accumulation of data harm consumer privacy. Businesses' attempts to protect user privacy can also have detrimental effects on competition. For example, the CMA recently accepted commitments from Google to address competition concerns arising from its Privacy Sandbox.[34] Likewise, the French Autorité de la concurrence is currentluy scrutinizing Apple's App Tracking Transparency Framework under French competition law.[35]

Finally, the Commission's draft DMA[36] explicitly integrates GDPR assessments into the conduct rules aimed at digital gatekeepers to make markets more contestable. Article 5(a) of the draft DMA prohibits designated gatekeepers from combining data collected from the core platform with data from other sources, unless the user has validly consented within the meaning of the GDPR. Effectively, this rule mirrors the approach of the Bundeskartellamt, although the DMA does not proclaim to protect consumers but competition by reducing the barriers to entry that vast data troves are thought to cause.[37] Will the Commission have to refer the question of whether consent was validly given to the national supervisory body of the Member State in which the gatekeeper is established before enforcing Article 5(a) against a gatekeeper platform? The DMA does not suggest such a procedure. It would also significantly undermine the effectiveness of the DMA, which intends to provide conduct rules that are quicker to enforce than classical competition law.

However, in order to make such a system work, there is a clear need for better and more regular interinstitutional cooperation between European data protection and competition agencies, both at the national and EU level.

06 CONCLUSION

Facebook v. Bundeskartellamt has the potential for a landmark ruling, not only for competition law but also for EU privacy regulation. It is unclear, however, whether the Court will wish to wade into the broader dispute on the type of harm competition law is meant to protect. This is an emotionally and ideologically charged topic, and hence the Court may well choose to avoid general pronouncements and limit itself to a narrow ruling on whether it is permissible for a competition agency to apply the GDPR for the purposes of assessing business conduct under the competition rules.

It is argued here that the Bundeskartellamt did not enforce the GDPR in a way that infringes the GDPR's enforcement system. The Bundeskartellamt interpreted national law in line with the principles and compromises the EU legislator struck when attempting to balance the competing interests of data protection, economic freedom and efficiency in the GDPR. Banning a public body from interpreting national law in line with the GDPR in cases that the competent data protection agency has not investigated would significantly undermine the effectiveness of the regulation. More generally, competition and data protection agencies working in institutional silos, without regard to the impact of their decisions on the other agency's objectives, risks yielding politically incoherent and hence undesirable results.

34 CMA, decision of February 11, 2022 to accept commitments offered by Google in relation to its Privacy Sandbox Proposals (Case number 50972).

35 Autorité de la concurrence, Decision 21-D-07 of March 17, 2021.

36 European Commission, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.

37 *Supra*, recital 36.

Regulating the activities of major digital platforms requires an interdisciplinary and interinstitutional approach. To this end, competition and privacy agencies should establish a system of regular dialogue and cooperation. The system set up by Regulation 1/2003 and the European Competition Network for the purposes of coordinating the enforcement of Articles 101 and 102 TFEU could serve as a useful blueprint for these purposes.

It is argued here that the Bundeskartellamt did not enforce the GDPR in a way that infringes the GDPR's enforcement system

---

CAN THE FTC PROMULGATE EFFECTIVE PRIVACY RULES?

BY
BEN ROSSEN

Mr. Rossen is Special Counsel in the Antitrust & Competition Law Practice Group of Baker Botts LLP and a former senior attorney in the FTC's Division of Privacy and Identity Protection. The views presented in this paper are those of the author and do not necessarily reflect the views of the firm or any client.

01 INTRODUCTION

When the Federal Trade Commission ("FTC") announced in December that it is considering commencing a "commercial surveillance" rulemaking to "curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination,"[2] privacy advocates appeared to have cause for celebration. Finally, after years of stalled negotiations on comprehensive privacy legislation in Congress, a newly aggressive FTC under Chair Lina Khan was going to blow the dust off the Commission's musty old rulemaking powers and solve America's privacy problem once and for all.

2 https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69.

Unfortunately, the truth is a bit more nuanced. While the FTC has considerable power to make rules prescribing unfair and deceptive acts and practices ("UDAP") under Section 18 of the FTC Act (so-called "Magnuson-Moss" rulemaking after the Magnuson-Moss Warranty – Federal Trade Commission Improvement Act of 1975), there are also significant drawbacks to this authority that may make it a poor fit for privacy regulation. Magnuson-Moss rulemaking is far from costless: it is slow and burdensome, and complicated privacy rules will likely take years to complete. It will also require the FTC to devote significant resources to rulemaking, likely at the expense of enforcement. From a policy perspective, Magnuson-Moss will force the FTC to shoehorn every privacy issue into the FTC Act's definition of unfairness, which can be difficult when informational injuries can be quite subjective. There are also real questions as to whether FTC rulemaking is the right solution at all for a problem as complex as data privacy where most stakeholders generally agree that Congress is better suited than unelected Commissioners to resolve the difficult policy trade-offs necessary for effective regulation.

Chair Khan has also hinted that the FTC may engage in competition rulemaking under Section 6(g) of the FTC Act to regulate "the abuses stemming from surveillance-based business models" because "it is not only consumers that are threatened by [such business models] but also competition."[3] Unfair methods of competition ("UMC") rulemaking under Section 6(g) could theoretically be achieved through notice-and-comment rulemaking under the Administrative Procedure Act, a much faster process than Magnuson-Moss. But there are serious questions as to whether the FTC has any authority to issue competition rules, guaranteeing a legal challenge that would likely end poorly for the agency.

> ***Privacy, however, will be a different story and no easy road for the Commission***

Nonetheless, the FTC appears ready to invest heavily in rulemaking. In March 2021, then-Acting Chairwoman Rebecca Slaughter announced a new rulemaking group within the FTC's Office of the General Counsel that would be tasked with streamlining the FTC's "planning, development, and execution" of new rules intended to "deliver effective deterrence for the novel harms of the digital economy and persistent old scams alike."[4] One of Khan's first actions as Chair was to approve changes to the Commission's procedures to "streamline" Magnuson-Moss rulemaking proceedings while giving the Chair and a majority of Commissioners more direct control over the process. Since then, the FTC has issued advance notices of proposed rulemaking for two new UDAP rules: a rule prohibiting business and government impersonation fraud and a rule prohibiting unfair or deceptive earnings claims. These two rules both received bipartisan support and were adopted unanimously, in part because they address relatively uncontroversial deceptive practices.

Privacy, however, will be a different story and no easy road for the Commission. This article addresses some of the reasons why FTC rulemaking is ultimately a poor substitute for federal legislation and, likely, an inefficient allocation of limited agency resources.

02

HOW WE GOT HERE: THE CASE FOR FTC RULEMAKING

The FTC has served as America's *de facto* privacy regulator since the passage of the Fair Credit Reporting Act in the 1970s. Under Section 5 of the FTC Act, which prohibits unfair and deceptive commercial practices, the FTC has pursued privacy and data security cases in myriad areas across the digital economy. But the FTC Act was never designed to be a privacy statute and a UDAP framework, while broad and flexible, is not always a good fit for privacy and data security. Many of the FTC's early cases in this area focused on deception, which requires the agency to show that a representation, omission, or practice is likely to mislead consumers acting reasonably under the circumstances, and that it is material – that is, it would likely affect a consumer's conduct or decisions with regard to a product or service.[5] The FTC regularly used this authority to challenge deceptive claims in privacy policies – which the agency deems to be "material" despite the fact that few consumers read them. While the FTC has brought

3 Federal Trade Comm'n, Statement of Regulatory Priorities at 2, https://www.reginfo.gov/public/jsp/eAgenda/StaticContent/202110/Statement_3084_FTC.pdf.

4 Fed. Trade Comm'n, *FTC Acting Chairwoman Slaughter Announces New Rulemaking Group* (Mar. 25, 2021), https://www.ftc.gov/news-events/press-releases/2021/03/ftc-acting-chairwoman-slaughter-announces-new-rulemaking-group.

5 See FTC Policy Statement on Deception (Oct. 23, 1984) (appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 183 (1984)), https://www.ftc.gov/public-statements/1983/10/ftc-poliystatement-deception.

some important deception cases, the upshot of these efforts was that companies learned to say very little about their privacy practices.

Unfairness, meanwhile, requires proof that an act or practice (1) causes or is likely to cause substantial injury, (2) that is not reasonably avoidable by consumers themselves, and (3) is not outweighed by benefits to consumers or competition.[6] The FTC has long recognized that unjustified, substantial consumer injury is the primary focus of the FTC Act, and not all injuries are legally "unfair."[7] Historically, substantial injury meant financial harm or serious threats to health and safety, and the FTC's longstanding policy statement provides that "[e]motional impact, and other more subjective types of harm . . . will not ordinarily make a practice unfair."[8] Similarly, by statute, public policy considerations cannot serve as the primary basis for a finding of unfairness. These requirements pose challenges for aggressive privacy enforcement against practices like targeted advertising where reasonable people can and do disagree about the extent of injury and there are significant countervailing benefits from free online services. Nonetheless, the FTC has wielded its unfairness authority to stop a variety of harmful practices, including failures to reasonably secure personal information,[9] soliciting and publicly posting nonconsensual pornography along with victims' personal information,[10] selling sensitive data such as Social Security numbers to third parties that did not have a legitimate business need for the information,[11] and collecting and sharing sensitive television-viewing information without notice or consent,[12] among others.

The limitations of the FTC's UDAP authority have grown more apparent with the rise of the tech giants and increasing calls for aggressive regulation. Recognizing these limitations, Commissioners from both sides of the aisle have repeatedly urged Congress to enact comprehensive privacy legislation that would establish baseline privacy protections for all Americans, give the FTC stronger teeth to enforce it through civil penalty authority for first-time offenses, and authorize the FTC to hire more attorneys and technologists to enforce the law.

Nonetheless, Congress has failed to act. Despite a growing patchwork of state privacy laws that prompted industry to come to the table in favor of federal legislation – and, specifically, preemption – the prospects of federal legislation remain dim. Increasingly, privacy advocates and members of Congress have called on the FTC to enact privacy rules instead.[13] Somewhat surprisingly, even Republican Commissioner Christine Wilson – no fan of rulemaking – reluctantly voiced her support for privacy rulemaking last year (which she has since walked back) to solve the "market failure" caused by information asymmetries among consumers and the companies that collect, use, and share consumer personal information. Alvaro Bedoya, likely to be confirmed as a fifth commissioner soon, has previously indicated that he would support privacy rulemaking[14] and it thus appears likely the FTC will move quickly to start the process once he arrives.

> ***"The FTC has long recognized that unjustified, substantial consumer injury is the primary focus of the FTC Act, and not all injuries are legally "unfair."***

6 15 U.S.C. § 45(n).

7 See FTC Policy Statement on Unfairness (Dec. 17, 1980) (appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

8 *Id.*

9 See e.g. *In the Matter of InfoTrax Systems, L.C.,* FTC File No. 162 3130, Docket No. C-4696 (2019); *FTC v. Equifax*, No. 1:19-cv-03927-TWT (N.D. Ga. 2019).

10 FTC v. EMP Media, Inc. (d/b/a MyEx.com), No. 2:18-cv-00035 (D. Nev. 2018); *In the Matter of Craig Brittain*, FTC File No. 132 3120, Docket No. C-4564 (2015).

11 *FTC v. Sitesearch Corp. d/b/a LeapLab*, No. 2:14-cv-02750 (D. Ariz. Feb. 18, 2016).

12 *FTC v. Vizio, Inc.,* No. 2:17-cv-00758 (D.N.J. 2017).

13 See Letter from Sen. Richard Blumenthal, et al., to the Hon. Lina Khan, Chair, Federal Trade Commission (Sep. 21, 2021), https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf.

14 S&P Global Market Intelligence, *FTC nominee signals support for privacy rules, Big Tech regulations* (Nov. 17, 2021), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/ftc-nominee-signals-support-for-privacy-rules-big-tech-regulations-67645909.

03

IS MAGNUSON-MOSS RULEMAKING WORTH ALL THE EFFORT?

The most likely source of authority for privacy rulemaking is Section 18 of the FTC Act, which authorizes the agency to enact "rules that define with specificity" unfair or deceptive acts or practices in or affecting commerce. This would be the most logical route because the FTC has always treated privacy as a consumer protection issue and Congress has unambiguously delegated this authority to the FTC through Magnuson-Moss. Section 18 rulemaking would give the FTC considerable – though not unlimited – flexibility to declare a variety of privacy or security concerns to be "an unfair act or practice" under the FTC Act.

However, Magnuson-Moss rulemaking is far from costless. First, it imposes significant burdens on limited agency resources. Despite recent attempts by the FTC to streamline rulemaking procedures under Magnuson-Moss,[15] it remains a slow, byzantine process that requires the agency to navigate a maze of bureaucratic obstacles before a final rule can become effective. The statute is particularly burdensome when it comes to complex or controversial rules, which could include dozens of mandates – each of which the FTC would need to prove addresses an unfair or deceptive practice, as defined by statute and agency guidance, that is "prevalent" in the market. It requires the FTC to hold adjudicative hearings with cross-examination and rights of rebuttal, and respond to all significant comments, proposed regulatory alternatives, and requests for exemptions. While the agency can place some limits on the extent of due process afforded to interested parties, anyone can challenge the rule on appeal if the FTC's limits on cross-examination or rebuttal precluded disclosure of disputed material facts. A complex set of privacy and security rules would likely take years to become final. Without bipartisan consensus, a new administration could simply cancel unfinished rulemaking, potentially wasting years of effort. In the meantime, how many cases would the FTC have been able to bring if it instead focused its resources on aggressive enforcement?

Second, although there are many ways that the FTC could try to formulate rules that restrict data collection and use, the FTC's authority to promulgate UDAP rules is limited to practices that are unfair or deceptive under the FTC Act, which, as previously discussed, does not always track neatly with privacy. It may therefore be difficult for the FTC to promulgate sweeping rules prohibiting behavioral advertising without a foundation that such practices are already recognized as unfair. It would also be difficult for the FTC to prohibit consumers from consenting to certain uses of data because an act or practice can only be unfair under the FTC Act if it was not reasonably avoidable by consumers themselves, such as through clear and conspicuous disclosures or meaningful consent. The FTC will likely identify a bevy of potential harms resulting from "commercial surveillance," such as an increased risk of data breaches, misinformation campaigns, social media's effects on children and teens, and discrimination caused by microtargeting of protected classes.[16] But if the FTC targets these harms with overbroad rules that simply ban digital advertising, the rulemaking record will be full of evidence of the benefits consumers receive from free ad-supported online services and the procompetitive effects of digital advertising on small publishers and niche brands that were able to flourish due to inexpensive customer acquisition through targeted ads. The FTC would need to explain why other less burdensome regulatory alternatives are inappropriate (such as opt-in consent or a universal opt-out regime), particularly when the FTC has itself repeatedly recognized the significant benefits to consumers from the collection and use of data. Challengers would undoubtedly use the FTC's past statements and guidance on appeal to try to invalidate the agency's rules or reopen the rulemaking record, all of which could result in further delay and cast doubt upon the validity of any final FTC rule.

> ***"The most likely source of authority for privacy rulemaking is Section 18 of the FTC Act, which authorizes the agency to enact "rules that define with specificity" unfair or deceptive acts or practices in or affecting commerce***

Finally, Magnuson-Moss rulemaking could further exacerbate the problem of patchwork compliance with privacy regulations because it is by no means clear to what extent such regulations would preempt state law. Califor-

15 See Fed. Trade Comm'n, *FTC Votes to Update Rulemaking Procedures, Sets Stage for Stronger Deterrence of Corporate Misconduct* (July 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-votes-update-rulemaking-procedures-sets-stage-stronger-deterrence-corporate-misconduct.

16 See e.g. *Wait But Why? Rethinking Assumptions About Surveillance Advertising*, IAPP Privacy Security Risk Closing Keynote 2021, Remarks of Commissioner Rebecca Slaughter (Oct. 22, 2021).

nia, Colorado, Virginia, and Utah have all recently enacted comprehensive privacy laws, and many other states are considering similar legislation. Federal privacy legislation that provides strong baseline privacy protections while establishing a national standard could streamline compliance costs for industry while providing significant benefits to consumers. By contrast, Magnuson-Moss does not contain any express preemption clause and implied preemption is by no means guaranteed.[17] The few cases to have considered the preemptive effect of Magnuson-Moss regulations suggest that the FTC could preempt state laws that pose a direct conflict or are inconsistent with particularized purposes of a detailed regulatory scheme,[18] but the law of "obstacle preemption" is far from settled and requires courts to divine legislative intent.[19] Thus, rather than creating a national standard, FTC regulations could result in competing federal and state privacy regimes, further complicating the patchwork of compliance.

> ***Magnuson-Moss rulemaking could further exacerbate the problem of patchwork compliance with privacy regulations because it is by no means clear to what extent such regulations would preempt state law***

In a best-case scenario, a Magnuson-Moss rulemaking might push Congress to finally pass much-needed federal privacy legislation. Alternatively, targeted rulemaking addressing egregious business practices that unquestionably injure consumers might receive bipartisan support, and relatively narrow rules could probably be completed in a year or less. On the other hand, a partisan rulemaking process that tries to mimic comprehensive legislation or ban entire industries would almost certainly result in a years-long slog, tying up limited agency resources with potentially little to show for it. And if history is any guide, agency overreach will not be received well in Congress, especially if political winds change. The end result of such a process is unlikely to justify the significant costs of rulemaking.

04

UMC RULEMAKING IS NOT AN APPROPRIATE REGULATORY SOLUTION

The FTC might also try to regulate privacy through competition rulemaking under Section 6(g) of the FTC Act, but this path is far riskier due to serious questions about the FTC's authority to promulgate substantive competition rules. Proponents of UMC rulemaking see Section 6(g) as a faster alternative to Magnuson-Moss because it would be governed by simple notice-and-comment rulemaking under the Administrative Procedure Act.[20]

Chair Khan, who has previously expressed her support for UMC rulemaking, has already begun to pave the way for it. For instance, in July 2021, the Commission rescinded, without replacing, its bipartisan Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act, opening the door to UMC enforcement that extends beyond the constraints of other antitrust laws. More recently, a December filing describing the agency's annual regulatory priorities stated that the FTC "in the coming year will consider developing . . . unfair-methods-of-competition rulemakings," specifically calling out "the abuses stemming from surveillance-based business models" as a particular concern of the Commission because of threats to both consumers *and* competition.[21]

17 See e.g. Alden Abbot, *Broad-Based FTC Data-Privacy and Security Rulemaking Would Flunk a Cost-Benefit Test*, Int'l Ctr. for L. & Econ. (Oct. 13, 2021), https://laweconcenter.org/resource/broad-based-ftc-data-privacy-and-security-rulemaking-would-flunk-a-cost-benefit-test/.

18 See *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 990-91 (D.C. 1984) (upholding conflict preemption of Credit Practices Rule where the FTC made clear the rule as not intended to occupy the field of credit regulation, and drafted the rule to be as consistent with state law as possible); *Katharine Gibbs Sch. Inc. v. FTC*, 612 F.2d 658, 667 (2d Cir. 1979) (invalidating overbroad preemption of the Vocational School Rule that preempted "any provision of any state law, rule, or regulations which is inconsistent with or otherwise frustrates the purpose of the provisions of this trade regulation rule.").

19 See generally *Federal Preemption: A Legal Primer,* Cong. Research Serv. (July 23, 2019), at 28, https://sgp.fas.org/crs/misc/R45825.pdf.

20 See e.g. Rohit Chopra & Lina Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. Chi. L. Rev. 357 (2020).

21 Federal Trade Comm'n, Statement of Regulatory Priorities at 2, https://www.reginfo.gov/public/jsp/eAgenda/StaticContent/202110/Statement_3084_FTC.pdf.

As I and others have written about elsewhere, broad UMC rulemaking would be a terrible strategic error for the FTC.[22] Substantive rulemaking under Section 6(g) stands on shaky legal footing, at best. UMC rulemaking proponents point to *National Petroleum Refiners Association v. FTC*, a 1973 D.C. Circuit case that upheld the FTC's authority to issue broad legislative rules under the FTC Act, and the only court to have considered the FTC's UMC rulemaking power.[23] They argue that Congress effectively ratified *National Petroleum Refiners* when it enacted detailed UDAP rulemaking provisions in Magnuson-Moss without addressing UMC, and that the FTC's determination that a practice is a UMC will receive *Chevron* deference.

The premise of this argument is fundamentally incorrect. While a detailed analysis of *National Petroleum Refiners* is beyond the scope of this paper, suffice it to say that it is highly unlikely that any modern court would similarly interpret the FTC Act. The D.C. Circuit's permissive statutory analysis effectively concluded that an ambiguous grant of rulemaking authority should be construed to give agencies the broadest possible powers so that they will have flexibility in determining how to effectuate their statutory mandates. Not only has the Supreme Court never explicitly adopted this approach, recent decisions under the major questions doctrine strongly suggest it would decline to do so if presented the opportunity.[24] Some scholars have gone so far as to argue that no current Supreme Court justice would approach statutory interpretation the way the D.C. Circuit did in *National Petroleum Refiners*.

"The premise of this argument is fundamentally incorrect. While a detailed analysis of National Petroleum Refiners is beyond the scope of this paper, suffice it to say that it is highly unlikely that any modern court would similarly interpret the FTC Act.

UMC rulemaking would be an especially poor fit for privacy given that only the FTC has authority to enforce Section 5 of the FTC Act but antitrust enforcement is divided between the FTC and the Department of Justice. This would lead to obvious problems if, for example, the FTC banned behavioral advertising as UMC: companies subject to FTC oversight would then face *per se* liability, while those overseen by DOJ would have the exact same practices evaluated under a rule of reason analysis. Consider, for example, the absurd results that would stem from how DOJ and FTC have divided enforcement among the biggest tech companies, with the FTC handling Meta and Amazon but DOJ overseeing Google and Apple.

For all these reasons, the FTC would be foolhardy to tackle privacy through UMC rules when Magnuson-Moss, despite its drawbacks, provides clear authority to promulgate UDAP rules, does not present issues of divided enforcement, and is far more consistent with the FTC's longstanding approach to privacy under its consumer protection authority.

05
CONCLUSION

Privacy regulation, if successful, could prove to be the defining consumer protection achievement of Lina Khan's tenure as Chair of the FTC. But this outcome is far from a certainty. Privacy rulemaking will be slow and inefficient, and at the end of the day, may not even produce enforceable final rules. While some have opined that the FTC must enact privacy rules soon because the worst possible outcome would be that neither Congress nor the FTC act to protect Americans' privacy, there are arguably worse outcomes. Setting aside the possibility of Congressional blowback reminiscent of the FTC's darkest days after *KidVid*, failed rulemaking that siphons the agency's limited resources away from case-by-case enforcement could leave consumers less protected than ever. If, as expected, the FTC commences privacy rulemaking this year, the Commission should focus its efforts on the most egregious practices that plainly fit within the rubric of unfair-

22 See e.g. Maureen K. Ohlhausen & Ben Rossen, Dead End Road: National Petroleum Refiners Association and FTC "Unfair Methods of Competition" Rulemaking, The FTC's Rulemaking Authority, Concurrences (forthcoming 2022); see also Maureen K. Ohlhausen & James Rill, *Pushing the Limits? A Primer on FTC Competition Rulemaking*, U.S. Chamber of Com. (Aug. 12, 2021), https://www.uschamber.com/assets/archived/images/ftc_rulemaking_white_paper_aug12.pdf.

23 482 F.2d 673 (D.C. Cir 1973).

24 See e.g. *Nat'l Fed'n of Indep. Bus. v. Dep't of Lab., Occupational Safety & Health Admin.*, 142 S. Ct. 661, 665 (2022) (*per curiam*).

ness and would be wise to avoid the distraction of UMC rules.

> *UMC rulemaking would be an especially poor fit for privacy given that only the FTC has authority to enforce Section 5 of the FTC Act but antitrust enforcement is divided between the FTC and the Department of Justice*


mod = modifier_ob.modifiers.new("
object to mirror_ob
mod.mirror_object = mirror_ob
ation == "MIRROR_X":
mod.use_x = True
mod.use_y = False
mod.use_z = False
ation == "MIRROR_Y":
mod.use_x = False
mod.use_y = True
mod.use_z = False
ation == "MIRROR_Z":
mod.use_x = False
mod.use_y = False
mod.use_z = True
ction at the end -add back the desel
.select= 1
.select=1
t.scene.objects.active = modifier_
lected" + str(modifier_ob)) # modifi
r_ob.select = 0
.context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES ----------
.Operator):
mirror to the selected object"""
t.mirror_mirror_x"
r X"
ntext):
t.active_object is not None

THE FTC SAFEGUARDS RULE: INFORMATION SECURITY PROGRAM ELEMENTS

BY
MELISSA J. KRASNOW

Melissa Krasnow is a partner at VLP Law Group LLP, Minneapolis, and an International Association of Privacy Professionals Certified Information Privacy Professional/US (CIPP/US).

01 INTRODUCTION

The federal and state law requirements for information security programs continue to evolve. Examples include the Federal Trade Commission ("FTC") Final Rule regarding Standards for Safeguarding Customer Information (the "FTC Rule") and the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (collectively, the "NY DFS Requirements").[2] This article describes the elements of an information security program under the FTC Rule and highlights differences between these elements with counterparts under the NY DFS Requirements. Financial institutions to which the FTC

2 86 Fed. Reg. 70,272 et seq. (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314) and 23 NYCRR pt. 500.

Rule applies should assess the extent to which their information security programs (for example, employee coordinators, risk assessments, safeguards, testing, service provider oversight and evaluation and adjustment, among other things), satisfy the elements of an information security program under the FTC Rule, identify, and address any gaps and document the foregoing. Others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law requirements for information security programs.

02
APPLICATION

The FTC Rule applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction.[3] *Financial institution* means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k).[4] An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.[5] Financial institutions include, without limitation, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission and entities acting as finders.[6] *Customer information* means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.[7] *Nonpublic personal information* means personally identifiable financial information and any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.[8] *Personally identifiable financial information* means any information that a consumer provides to the financial institution to obtain a financial product or service therefrom, about a consumer resulting from any transaction involving a financial product or service between the financial institution and a consumer or that the financial institution otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.[9] In addition to defining financial institution, customer information, nonpublic personal information, and personally identifiable financial information, the FTC Rule also defines authorized user, consumer, customer, encryption, financial product or service, financial service, information security program, information system, multifactor authentication, penetration testing, security event and service provider, among other things.[10]

> ***The FTC Rule applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction***

The NY DFS Requirements apply to a covered entity, meaning any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York Banking Law, the New York Insurance Law or the New York Financial Services Law.[11] *Nonpublic information* under the NY DFS Requirements means all electronic information that is not publicly available information and is: (1) business related information of a covered entity the tampering with which, or unauthorized disclosure, access

3 16 CFR § 314.1(b).

4 16 CFR § 314.2(h)(1).

5 16 CFR § 314.2(h)(1).

6 16 CFR § 314.1(b).

7 16 CFR § 314.2(d).

8 16 CFR § 314.2(l)(1).

9 16 CFR § 314.2(n)(1).

10 16 CFR § 314.2.

11 23 NYCRR § 500.1(c).

or use of which, would cause a material adverse impact to the business, operations or security of the covered entity, (2) any information concerning an individual which because of name, number, personal mark or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account or (v) biometric records, (3) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to: (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual or (iii) payment for the provision of health care to any individual.[12] In addition to defining a covered entity and nonpublic information, NY DFS Requirements also define cybersecurity event, information system, multi-factor authentication, risk assessment, risk-based authentication and third party service provider(s), among other things.[13]

03
INFORMATION SECURITY PROGRAM ELEMENTS

FTC Rule information security program elements include a qualified individual, risk assessments, safeguards, testing, training and personnel, oversight of service providers, evaluation and adjustment, an incident response plan and board reporting.[14] Certain of these elements do not apply to financial institutions that maintain customer information concerning fewer than 5,000 consumers ("Excepted Financial Institutions") as described below.[15] The NY DFS Requirements contain a number of exemptions (i.e. 23 NYCRR § 500.19).[16]

Although the FTC Rule became effective January 10, 2022, certain information security program elements become effective as of December 9, 2022 as described below.[17]

> ***"FTC Rule information security program elements include a qualified individual, risk assessments, safeguards, testing, training and personnel, oversight of service providers, evaluation and adjustment, an incident response plan and board reporting***

A. Qualified Individual

Under the FTC Rule, a qualified individual (not limited to the Chief Information Security Officer ("CISO"), as required by the NY DFS Requirements) that is responsible for overseeing, implementing, and enforcing the information security program ("Qualified Individual") must be designated.[18] The foregoing becomes effective as of December 9, 2022.[19]

B. Risk Assessments

The FTC Rule requires the information security program to be based on a written risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and that assesses the sufficiency of any safeguards in place to control these risks and must include criteria and requirements as follows, except for Excepted Financial Institutions.[20] The criteria and requirements must include: criteria for the evaluation and categorization of identified security risks or threats that the financial institution faces, criteria for the assessment of the confidenti-

12 23 NYCRR § 500.1(g).

13 23 NYCRR § 500.1.

14 16 CFR § 314.4.

15 16 CFR § 314.6.

16 23 NYCRR § 500.19.

17 86 Fed. Reg. 70,272 et seq. (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314).

18 16 CFR § 314.4(a) and 23 NYCRR § 500.4(a).

19 16 CFR § 314.5.

20 16 CFR § 314.4(b)(1) and 16 CFR § 314.6.

ality, integrity and availability of the financial institution's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats the financial institution faces, and requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.[21] The foregoing becomes effective as of December 9, 2022.[22] Also, additional risk assessments must be performed periodically.[23]

> *The FTC Rule requires the information security program to be based on a written risk assessment that identifies reasonably foreseeable internal and external risks to the security*

The NY DFS Requirements require periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program, carried out in accordance with written policies and procedures, which must be documented and updated as reasonably necessary to address changes to such information systems, nonpublic information or business operations, allow for revision of controls to respond to technological developments and evolving threats and consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems.[24]

C. Safeguards

The FTC Rule requires safeguards to control the risks identified through risk assessment to be designed and implemented, which become effective as of December 9, 2022, as follows.[25]

Access Controls. Under the FTC Rule, access controls must be implemented and periodically reviewed access controls, including technical and, as appropriate, physical controls to: authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information and limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information.[26] As part of a cybersecurity program under the NY DFS Requirements, based on the risk assessment, user access privileges to information systems that provide access to nonpublic information must be limited and periodically reviewed.[27]

Identification and Management of Data, Personnel, Devices, Systems, and Facilities. The FTC Rule requires the data, personnel, devices, systems, and facilities that enable achievement of business purposes in accordance with their relative importance to business objectives and risk strategy to be identified and managed.[28]

Encryption. Under the FTC Rule, all customer information held or transmitted both in transit over external networks and at rest must be protected by encryption or, to the extent that encryption is determined to be infeasible, be secured using effective alternative compensating controls reviewed and approved by the Qualified Individual.[29] The FTC Rule defines *encryption as* the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.[30] As part of a cybersecurity program under the NY DFS Requirements, based on the risk assessment, controls, including encryption, must be implemented to protect nonpublic information and, to the extent that encryption of nonpublic information is determined to be infeasible, such nonpublic information must be secured using alternative compensating controls, which must be

21 16 CFR § 314.4(b)(1).

22 16 CFR § 314.5.

23 16 CFR § 314.4(b)(2).

24 23 NYCRR § 500.9(a)-(b).

25 16 CFR § 314.4(c) and 16 CFR § 314.5.

26 16 CFR § 314.4(c)(1).

27 23 NYCRR § 500.7.

28 16 CFR § 314.4(c)(2).

29 16 CFR § 314.4(c)(3).

30 16 CFR § 314.2(f).

reviewed and approved by the CISO.[31] To the extent utilized, the feasibility of encryption and effectiveness of the compensating controls must be reviewed by the CISO at least annually.[32]

Application Security. The FTC Rule requires secure development practices for in-house developed applications utilized for transmitting, accessing or storing customer information and procedures for evaluating, assessing or testing the security of externally developed applications utilized to transmit, access or store customer information to be adopted.[33] The NY DFS Requirements require a cybersecurity program to include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized and procedures for evaluating, assessing or testing the security of externally developed applications utilized within the context of the covered entity's technology environment and all such procedures, guidelines and standards must be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee).[34]

Multi-Factor Authentication. The FTC Rule requires multi-factor authentication for any individual accessing any information system to be implemented, unless the Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls.[35] The FTC Rule defines *multi-factor authentication* as authentication through verification of at least two of the following types of authentication factors: knowledge factors (such as a password), possession factors (such as a token) or inherence factors (such as biometric characteristics).[36]

The NY DFS Requirements define *multi-factor authentication* slightly differently from the FTC Rule: authentication through verification of at least two of the following types of authentication factors: knowledge factors (such as a password), possession factors (such as a token or text message on a mobile phone) or inherence factors (such as a biometric characteristic).[37] Multi-factor authentication must be utilized for any individual accessing internal networks from an external network, unless the CISO has approved in writing the use of reasonably equivalent or more secure access controls and, based on the risk assessment, effective controls, which may include multi-factor authentication or risk-based authentication, must be used to protect against unauthorized access to nonpublic information or information systems.[38]

> ***The FTC Rule requires multi-factor authentication for any individual accessing any information system to be implemented***

Data Disposal. Under the FTC Rule, procedures must be developed, implemented and maintained for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained and the financial institution's data retention policy must be periodically reviewed to minimize the unnecessary retention of data.[39] As part of a cybersecurity program under the NY DFS Requirements, there must be policies and procedures for the secure disposal on a periodic basis of nonpublic information under 23 NYCRR § 500.1(g)(2)-(3).[40]

Change Management. The FTC Rule requires adopting procedures for change management.[41]

31 23 NYCRR § 500.15(a).

32 23 NYCRR § 500.15(b).

33 16 CFR § 314.4(c)(4).

34 23 NYCRR § 500.8.

35 16 CFR § 314.4(c)(5).

36 16 CFR § 314.2(k).

37 23 NYCRR § 500.1(f).

38 23 NYCRR § 500.12.

39 16 CFR § 314.4(c)(6).

40 23 NYCRR § 500.13.

41 16 CFR § 314.4(c)(7).

Logging. Policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users must be implemented under the FTC Rule.[42] The NY DFS Requirements require such policies, procedures, and controls to be risk-based.[43]

> *The FTC Rule requires adopting procedures for change management*

D. Testing

The FTC Rule requires regular testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems and, for information systems, monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments.[44] The FTC Rule defines p*enetration testing* as a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside the financial institution's information systems (the NY DFS Requirements use the same definition regarding a covered entity).[45]

Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, the following must be conducted: annual penetration testing of the information systems determined each given year based on relevant identified risks in accordance with the risk assessment and vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in the information systems based on the risk assessment, at least every six months and whenever there are material changes to operations or business arrangements and whenever there are circumstances known or for which there is a reason to know may have a material impact on the information security program, except for Excepted Financial Institutions.[46] The foregoing becomes effective as of December 9, 2022.[47]

The NY DFS Requirements require the cybersecurity program for a covered entity to include monitoring and testing, developed in accordance with the risk assessment, designed to assess the effectiveness of the cybersecurity program, including continuous monitoring or periodic penetration testing and vulnerability assessments.[48] Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities, a covered entity must conduct annual penetration testing of the covered entity's information systems determined each given year based on relevant identified risks in accordance with the risk assessment and bi-annual vulnerability assessments, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the covered entity's information systems based on the risk assessment.[49]

E. Training and Personnel

The FTC Rule requires implementing policies and procedures to ensure that personnel are able to enact the information security program by: (1) providing personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment; (2) utilizing qualified information security personnel employed by the financial institution or an affiliate or service provider sufficient to manage information security risks and to perform or oversee the information security program; (3) providing information security personnel with security updates and training sufficient to address relevant security risks and (4) verifying that key information security personnel take steps to maintain current knowledge of changing informa-

42 16 CFR § 314.4(c)(8).

43 23 NYCRR § 500.14(a).

44 16 CFR § 314.4(d)(1).

45 16 CFR § 314.2(m) and 23 NYCRR § 500.1(h).

46 16 CFR § 314.4(d)(2) and 16 CFR § 314.6.

47 16 CFR § 314.5.

48 23 NYCRR § 500.5.

49 23 NYCRR § 500.5.

tion security threats and countermeasures.[50] The foregoing becomes effective as of December 9, 2022.[51] The NY DFS Requirements are comparable to the foregoing.[52]

F. Oversight of Service Providers

The FTC Rule requires oversight of service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.[53] The FTC Rule defines *service provider* as any person or entity that receives, maintains, processes or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to 16 CFR Part 314.[54] The FTC Rule also requires overseeing service providers by periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.[55] The foregoing becomes effective as of December 9, 2022.[56]

The NY DFS Requirements define *third party service provider* as a person that is not an affiliate of the covered entity, provides services to the covered entity and maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity.[57]

Subject to a specified exception, the NY DFS Requirements require implementing written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers, which must be based on the risk assessment, and address to the extent applicable: (1) identification and risk assessment of third party service providers, (2) minimum cybersecurity practices required to be met by such third party service providers in order for them to do business with the covered entity, (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third party service providers and (4) periodic assessment of such third party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.[58]

Such policies and procedures must include relevant guidelines for due diligence and/or contractual protections relating to third party service providers including to the extent applicable guidelines addressing: (1) the third party service provider's policies and procedures for access controls, including its use of multi-factor authentication as required by 23 NYCRR § 500.12, to limit access to relevant information systems and nonpublic information, (2) the third party service provider's policies and procedures for use of encryption as required by 23 NYCRR § 500.15 to protect nonpublic information in transit and at rest, (3) notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or nonpublic information being held by the third party service provider and (4) representations and warranties addressing the third party service provider's cybersecurity policies and procedures that relate to the security of the covered entity's information systems or nonpublic information.[59]

> ***The FTC Rule requires implementing policies and procedures to ensure that personnel are able to enact the information security program***

G. Evaluation and Adjustment

Under the FTC Rule, the information security program must be evaluated and adjusted in light of the results of the required testing and monitoring, any material changes to operations or business arrangements. the results of risk assessments or any other circumstances known or for which

50 16 CFR § 314.4(e).

51 16 CFR § 314.5.

52 23 NYCRR § 500.14 and § 500.10.

53 16 CFR § 314.4(f)(1)-(2).

54 16 CFR § 314.2(q).

55 16 CFR § 314.4(f)(3).

56 16 CFR § 314.5.

57 23 NYCRR § 500.1(n).

58 23 NYCRR § 500.11(a) and (c).

59 23 NYCRR § 500.11(b).

there is reason to know may have a material impact on the information security program.[60]

H. Incident Response Plan

The FTC Rule requires establishing a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity or availability of customer information in the financial institution's control and must address: (1) the goals of the incident response plan, (2) the internal processes for responding to a security event, (3) the definition of clear roles, responsibilities and levels of decision-making authority, (4) external and internal communications and information sharing, (5) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls, (6) documentation and reporting regarding security events and related incident response activities and (7) the evaluation and revision as necessary of the incident response plan following a security event, except for Excepted Financial Institutions.[61] The foregoing becomes effective as of December 9, 2022.[62]

As part of a cybersecurity program under the NY DFS Requirements, a written incident response plan (containing content comparable to the foregoing under the FTC Rule) must be established, designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the information systems or the continuing functionality of any aspect of business or operations.[63]

> ***The FTC Rule requires the Qualified Individual to report in writing, regularly and at least annually, to the board of directors or equivalent governing body***

I. Board Reporting

The FTC Rule requires the Qualified Individual to report in writing, regularly and at least annually, to the board of directors or equivalent governing body (if no such board or body exists, such report must be timely presented to a senior officer responsible for the information security program) and the report must include the following information: the overall status of the information security program and compliance with 16 CFR Part 314 and material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto and recommendations for changes in the information security program, except for Excepted Financial Institutions.[64]

The foregoing becomes effective as of December 9, 2022.[65] Under the NY DFS Requirements, the CISO must report in writing at least annually to the board of directors or equivalent governing body on the cybersecurity program and material cybersecurity risks (if no such board or body exists, such report must be timely presented to a senior officer responsible for the cybersecurity program).[66] The CISO must consider to the extent applicable: (1) the confidentiality of nonpublic information and the integrity and security of the covered entity's information systems, (2) the covered entity's cybersecurity policies and procedures, (3) material cybersecurity risks to the covered entity, (4) overall effectiveness of the cybersecurity program and (5) material cybersecurity events involving the covered entity during the time period addressed by the report.[67]

60 16 CFR § 314.4(g).

61 16 CFR § 314.4(h) and 16 CFR § 314.6.

62 16 CFR § 314.5.

63 23 NYCRR § 500.16.

64 16 CFR § 314.4(i) and 16 CFR § 314.6.

65 16 CFR § 314.5.

66 23 NYCRR § 500.4(b).

67 23 NYCRR § 500.4(b).

04
CONCLUSION

Considering the January 10, 2022 effective date of the FTC Rule and certain information security program elements becoming effective as of December 9, 2022, financial institutions to which the FTC Rule applies should assess the extent to which their information security programs satisfy the elements of an information security program under the FTC Rule, identify, and address any gaps and document the foregoing. Others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law requirements for information security programs.

Others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law requirements for information security programs

WHAT'S NEXT

For May 2022, we will feature a TechREG Chronicle focused on issues related to **FinTech**.

ANNOUNCEMENTS

CPI TechREG CHRONICLES June & July 2022

For June 2022, we will feature a TechREG Chronicle focused on issues related to **Content Regulation**. And in May we will cover **Gig Economy**.

Contributions to the TechREG Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI TechREG Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "TechREG Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers in any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

ABOUT US

Since 2006, **Competition Policy International** ("CPI") has provided comprehensive resources and continuing education for the global antitrust and competition policy community. Created and managed by leaders in the competition policy community, CPI and CPI TV deliver timely commentary and analysis on antitrust and global competition policy matters through a variety of events, media, and applications.

As of October 2021, CPI forms part of **What's Next Media & Analytics Company** and has teamed up with **PYMNTS**, a global leader for data, news, and insights on innovation in payments and the platforms powering the connected economy.

This partnership will reinforce both CPI's and PYMNTS' coverage of technology regulation, as jurisdictions worldwide tackle the regulation of digital businesses across the connected economy, including questions pertaining to BigTech, FinTech, crypto, healthcare, social media, AI, privacy, and more.

Our partnership is timely. The antitrust world is evolving, and new, specific rules are being developed to regulate the so-called "digital economy." A new wave of regulation will increasingly displace traditional antitrust laws insofar as they apply to certain classes of businesses, including payments, online commerce, and the management of social media and search.

This insight is reflected in the launch of the **TechREG** Chronicle, which brings all these aspects together — combining the strengths and expertise of both CPI and PYMNTS.

Continue reading CPI as we expand the scope of analysis and discussions beyond antitrust-related issues to include Tech Reg news and information, and we are excited for you, our readers, to join us on this journey.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

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.

CPI COMPETITION POLICY™ INTERNATIONAL