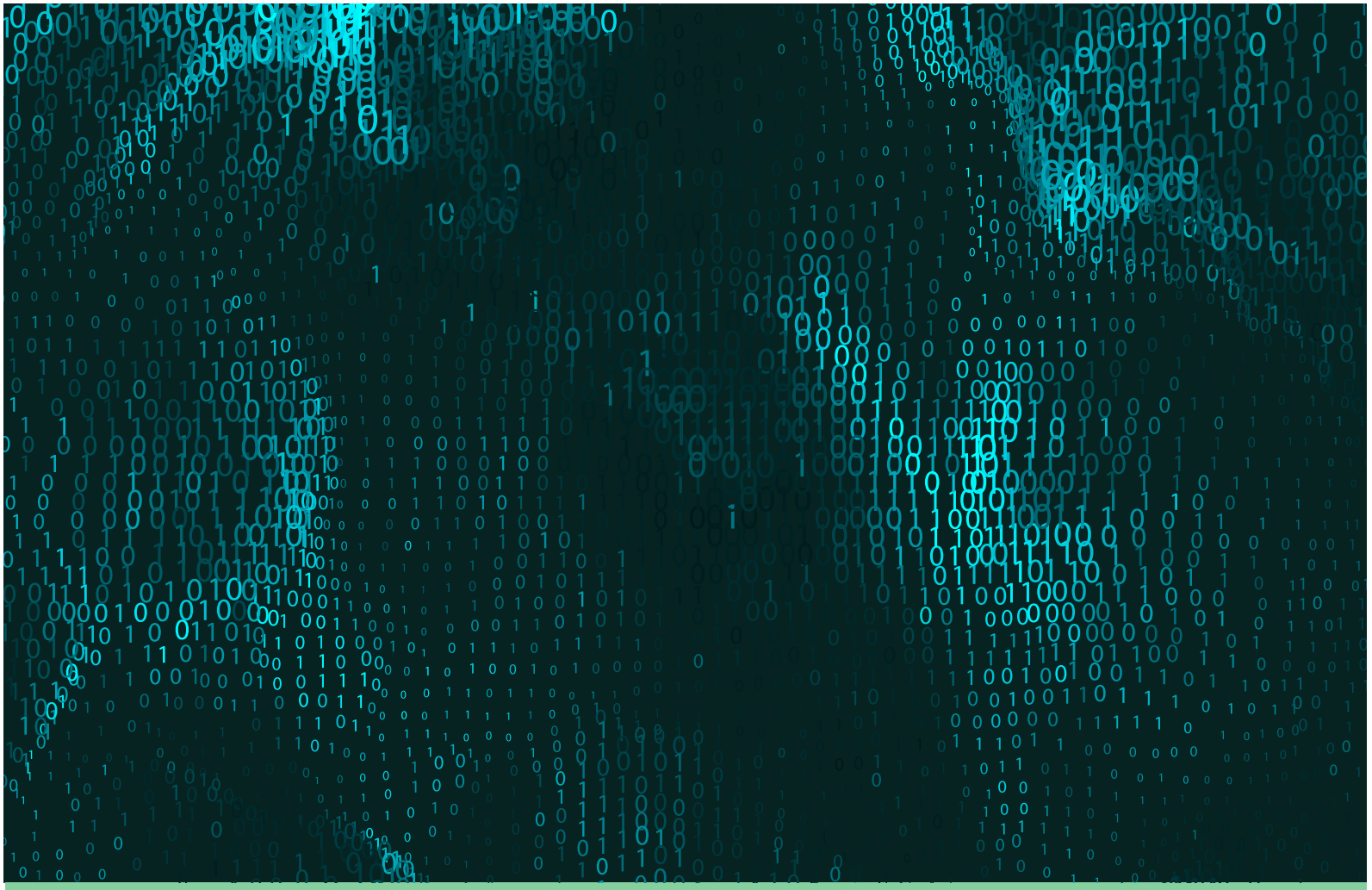

THE FUTURE OF PRIVACY REGULATION

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.

Visit www.competitionpolicyinternational.com for access to these articles and more!

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.

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.

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

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/.

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.

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 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

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).

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*

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 im-

portant 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 effec-

tive (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

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).

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 protections, 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***

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

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