fact generate larger societal effects. While the Executive Order is far from perfect,[10] it remains one of the most comprehensive U.S. foreign intelligence overhauls in history; certainly the first to be promulgated solely in response to external pressures and market demands that stem from such individual right claims. What Schrems was capable of doing, using the General Data Protection Regulation (GDPR) as his shield, should not be downplayed. He singlehandedly took down the biggest signals intelligence powerhouse in the world and forced it to reform its laws for the benefit of communities it did not previously cater to.

Look, I get it. We are all disenchanted with individual human rights law. We recognize that individual rights as a governing model comes with many, many flaws. Indeed, it is a myth to think there is some universal right to informational privacy or data protection, and the practice of states in the datasphere demonstrates just how frustrating the tension is between the mythical law in the books and the law in action. I also share Salomé's insightful concern about the collective harms that are generated by contemporary data markets. I just do not think we should be quick to reject the myth altogether as serving no purpose in this broader fight. Instead, I would invite Salomé to think more about transnational frameworks whereby we supplement our existing individual model with new collective approaches, without favoring one over the other. Such complementarity I think offers a better prescriptive solution to the current challenges we face in the datasphere.

Rebecca Hamilton

Thank you Asaf. Finally, Kirk, let us move to your presentation. No matter where in the world data regulation is taking place, there is an inevitable debate between taking a "sectoral approach" versus an "omnibus approach." To date, the United States seems to favor sectoral approaches. The European Union seems to be favoring omnibus approaches. Let us hear some concrete examples of the pros and cons of each approach. And is this sectoral versus omnibus the only way to think about this? What other options are out there?

Remarks by Kirk J. Nahra[11]

https://doi.org/10.1017/amp.2023.65

U.S. privacy law often is criticized in comparison with international privacy regimes, particularly the European Union's General Data Protection Regulation. Parts of this criticism are fair, but, at the same time, U.S. privacy law provides meaningful protections in a substantial set of circumstances, and, on occasion, provides either "better" privacy protection than the GDPR or presents a more targeted approach to balancing appropriate privacy protections with other important public policy concerns. This balancing often is not a question of "consumers vs. industry" (although it certainly can be). In some situations—particularly in the health care settings that I will focus on —it often is a question of providing an appropriate balance between privacy interests and other policy interests that benefit both industry and consumers.

[10] *See, e.g.*, Elizabeth Goiter, *The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance*, Just Security (Oct. 31, 2022), *at* https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance; Ashley Gorski, *The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance*, Just Security (Nov. 4, 2022), https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii.

[11] Kirk J. Nahra is a partner with WilmerHale in Washington, D.C., where he co-chairs the firm's Cybersecurity and Privacy Practice as well as the Big Data Practice. He teaches privacy law at the Washington College of Law at American University.

https://doi.org/10.1017/amp.2023.65 Published online by Cambridge University Press

GDPR provides (in a grossly simplistic summary) consistent protection for all personal data across all industries. There are no meaningful exceptions; it encompasses all kinds of data, from small and large companies, across all relevant industries. Some of the details of privacy compliance may vary based on relationships and purposes for processing data, but the idea is that there will be a single set of rules.[12]

The U.S. privacy model—as of this writing—is wildly different. U.S. privacy laws tend to fall into three categories. There are laws for specific industries.[13] There are laws dealing with specific data practices.[14] We also are seeing an increasing array of laws addressing particular data categories.[15] The result of this model is that we do not have one law in the United States, we have dozens. These laws provide tailored privacy protections in specific situations. Some of these protections are quite strong—at least if not more protective than the GDPR. Other areas provide lesser protection.

At the same time, with varying degrees of effectiveness, these laws are designed to provide privacy nuance, providing specific protections for specific activities. A positive of this approach is that privacy interests can be tailored to specific situations, rather than a generic "one size fits all" protection. At the same time, it is clear that this approach is extremely challenging for consumers to understand and increasingly difficult for businesses as well; the only short-term beneficiaries of this inconsistent, overlapping cornucopia are the growing number of privacy professionals across the country.

Let us explore this nuance. The best example stems from the privacy provisions of the HIPAA Privacy Rule. HIPAA's history is convoluted, and its privacy rule generates confusion. Contrary to common misperception, HIPAA is not an overall health information privacy law; instead, it protects certain information in certain contexts when that data is held by or otherwise connected to specific "covered entities" (primarily health plans/health insurers and health care providers), along with their service providers. Health information in other contexts simply is not covered by these rules.[16] You can certainly argue for a broader application of privacy protection for health information, but the drafters of the HIPAA Privacy Rule were stuck with their legislatively assigned scope.

With that scope, however, the regulatory drafters designed a privacy regime to provide very strong privacy protections for individual patients and insureds, while at the same time also allowing the health care system to work effectively and efficiently for the benefit of both individuals and the overall health care system. These policy choices have worked well (in my opinion), and can provide a model going forward for broader U.S. privacy law.

A few key choices in this policy debate. First, the drafters focused on the role of individual consent, navigating how best to allow for an individual role in the operation of the health care system and the protection of personal privacy. The regulatory choice is unusual (and perhaps unique) at

[12] GDPR does provide "special categories" of personal data, where additional obligations apply—with these special categories including data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." GDPR, Art. 9.

[13] See, e.g., the Health Insurance Portability and Accountability Act privacy and security regulations for the health care industry, the Gramm-Leach-Bliley Act for financial institutions, and the Family Educational Rights and Privacy Act for education.

[14] See, e.g., Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM) for email marketing and the Telephone Consumer Protection Act (TCPA) for telemarketing.

[15] Examples include: genetic data; biometric data; data about children; and even a specific law for video rental records.

[16] *See* Kirk Nahra, *A Public Service Announcement About the HIPAA Privacy Rule*, IAPP (June 18, 2021), *at* https://iapp.org/news/a/a-public-service-announcement-about-the-hipaa-privacy-rule/?mkt_tok=MTM4LUVaTS0wNDIAAAF9vwpQ5J6owEywaEB1Li1TO4b9svqYwNyX-naHSZYm-6qIK9So0uZt_UHYthr2MuDbwco1LDwS1ZsTet8TjnA4-26BuYX49G9I-6atGnn1kv_H.

https://doi.org/10.1017/amp.2023.65 Published online by Cambridge University Press

this point in U.S. privacy law. The drafters defined certain "common" or "expected" uses and disclosures of health information and defined the rules to make these normal uses and disclosures essentially automatic, with no individual consent actually required.

The rules also specify certain national priority areas where individual consent may be defined in a small series of targeted mini-rules. For all other uses and disclosures an individual authorization is required, which is a meaningful form of individual permission, subject to very specific standards.

The result of this approach—coupled with other compliance obligations imposed on the covered entities—is that the normal elements of the health care system proceed automatically, and only additional items require specific patient permission. This approach takes out the need for a patient to consent to each individual use and disclosure of their health information (which would likely require either a constant barrage of permission requests or an "automatic and largely meaningless approval of everything through a generic privacy notice). It imposes obligations automatically on covered entities, allows the normal activities to proceed efficiently, and focuses individual attention on only those unusual uses that require individual authorization.[17]

This model may be useful in debates over privacy law. An approach that would define appropriate uses and disclosures of personal could reduce the impact of unread and confusing privacy notices, while still creating substantive limitations on how personal data is being used.[18] At the same time, thinking about how to address health information in a national privacy law creates a broad array of challenges.[19]

Moving forward, as we grapple with not only "traditional" data privacy issues but also the role of artificial intelligence and the "collective" privacy issues addressed in Salomé's presentation here, these nuanced privacy approaches need to be evaluated, along with the broader but more generic approaches laid out in the GDPR and (increasingly) in the various "comprehensive" state laws being implemented across the United States. We certainly can improve current privacy law in the United States, primarily by addressing the large current gaps that exist in our complicated structure, but we may sacrifice some of the nuance in the law that provides meaningful benefits if we move to a single overall approach.

[17] *See generally* Kirk Nahra & Lydia Lichlyter, *Federal Privacy Legislation Should Be Context-Sensitive*, LAW360 (Feb. 27, 2020), *at* https://www.law360.com/articles/1248149.

[18] *See, e.g.*, Woodrow Hartzog & Neil M. Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFL. 356 (2022).

[19] *See* Kirk Nahra, *Healthcare in the National Privacy Law Debate*, 16 ABA HEALTH ESOURCE (Dec. 2019), *at* https://www.wilmerhale.com/en/insights/publications/20200114-healthcare-in-the-national-privacy-law-debate.

https://doi.org/10.1017/amp.2023.65 Published online by Cambridge University Press