# FOREWORD

Kelsey L. Kenny, J.D., CIPP/US[*] & Scott Bloomberg, J.D.[**]

## I. WHY A *STUDENT* JOURNAL OF INFORMATION PRIVACY LAW?

Welcome to the first paginated edition of the Student Journal of Information Privacy Law (SJIPL). A group of students at the University of Maine School of Law founded the SJIPL during the fall 2021 semester with the aim of establishing an outlet for student-authored scholarship about information privacy law. Following its formation, the Journal began publishing monthly editions comprised of shorter-form blog posts and more formal academic papers. The Maine Law faculty voted to formally recognize the SJIPL as the school's third law journal in fall 2022, and the Journal's editorial staff began working towards publishing its inaugural paginated edition shortly thereafter. This first volume was produced by a team of five hard-working editors. The authors of this Foreword served as Student Advisor and Faculty Advisor, respectively, to the Journal's editorial team.

At the outset, it is important to explain why we believe a *student* journal of information privacy law—that is, a journal publishing exclusively *student*-authored work—is needed at this point in time.

First and foremost, the rise of data-driven technologies in the modern digital economy has made information privacy law an extraordinarily important field of study. Indeed, the mid-century computer data-basing technologies that scholars like Alan Westin feared would intrude on individual privacy seem downright quaint in an era of smart devices, social media, extended reality, automated decision-making, and generative AI.[1] These technologies and many others that we use in our daily lives rely in large part upon collecting, storing, using, and sharing personal information. And, unfortunately, companies and governments that use these technologies have repeatedly fallen short in safeguarding our privacy, too often prioritizing competing interests like profit maximization over the best interests of individuals and society.

Take in-home smart devices for example. Internet-connected smart devices like cameras, thermostats, televisions, vacuums, and even refrigerators may carry significant benefits for users.[2] However, such devices also expose consumers to vulnerability by discretely generating countless data points about how their households operate on a daily basis.[3] The companies providing these devices can

* Graduate, Class of 2023, University of Maine School of Law and IAPP Westin Scholar.

** Associate Professor of Law and Director of the Information Privacy Law Certificate Program, University of Maine School of Law.

1. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

2. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 8-9 (2015) (highlighting some benefits of in-home smart devices); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 108-10 (2014) (providing early examples of in-home smart devices).

3. FED. TRADE COMM'N, *supra* note 2, at 14 (reporting that one company's in-home smart device generates a discrete data point every six seconds).

then use the data for secondary purposes that do not benefit consumers, such as selling it to data brokers or marketers.[4] Smart devices raise privacy-related cybersecurity issues as well. They can be hacked and create the potential for covert surveillance by bad actors.[5] Such unauthorized access could facilitate identity theft, burglary, or even physical assault.[6] And, the troves of data created by smart devices may be fertile ground for governments seeking to surveil or investigate citizens.[7]

Smart devices are just one example in a web of technologies that, if left unchecked, can be exploited in our surveillance capitalism economic system.[8] Attempting to provide that check through law has become a priority for regulators across the world, leading to a drastic expansion in the amount of privacy laws on the books. Globally, the most significant law is the European Union's General Data Protection Regulation (GDPR), which imposes stringent privacy obligations on entities within the EU and those seeking to do business with EU persons.[9] Since the GDPR's implementation in 2018, several other major economies, including China and Brazil, have enacted similar comprehensive privacy regimes.[10]

The United States, of course, has thus far failed to follow the EU's lead. We have no comprehensive federal privacy law. Nonetheless, an alphabet soup of sector-specific and state-level privacy laws has emerged to provide some protection for individual privacy. Federal laws such as HIPAA,[11] GLBA,[12] FCRA,[13] and FERPA[14] govern personal information used in specific sectors of the economy (health insurance, financial, consumer reporting, and educational contexts,

---

4. *See, e.g.*, Paul Ohm & Nathaniel Kim, *Legacy Switches: A Proposal to Protect Privacy, Security, and the Environment from the Internet of Things*, 84 OHIO ST. L. J. 101, 110-18 (2023) (summarizing privacy risks posed by smart devices).

5. *Id.*

6. *Id.*

7. *See, e.g.*, Andrew G. Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 560 (2017) ("The flip side of wonderfully revealing data trails for consumer insights is that those same digital fingerprints can also be used for government investigation. Police entrusted to prevent crime have recognized the value of digital surveillance. As the Internet of Things grows, the data trails from these smart devices will become increasingly helpful to law enforcement.").

8. *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019) (describing the "surveillance capitalism" economic system through which corporations exploit user data to predict and manipulate user behavior).

9. *See* Commission Regulation 2016/679 of the European Parliament and of the Council of Apr. 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 O.J. (L 119) (EU).

10. *See, e.g.*, IAPP, *Global Comprehensive Privacy Law Mapping Chart* https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/ (last updated Apr., 2022).

11. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C. §§ 18, 26, 29); *see also* HIPAA Privacy Rule, 45 C.F.R. §§ 160, *et seq.* (2020).

12. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in relevant part at 15 U.S.C. §§ 6801-6809, 6821-6827).

13. Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. §§ 1681, *et seq*.).

14. Family Educational Rights and Privacy Act, Pub. L. 93-380, 88 Stat. 484 (1974) (codified as amended at 20 U.S.C. § 1232g).

respectively). Other federal laws like COPPA[15] and Section Five of the FTC Act[16] apply across industries but only protect certain persons (children who use the internet, in the case of COPPA) or prohibit certain practices (unfair and deceptive acts, in the case of Section Five). On the state side, California led the way by enacting its comprehensive privacy law, the CCPA, via ballot initiative in 2018 and then expanding the protections offered by that law in 2020.[17] Virginia, Colorado, Connecticut, Utah, and Iowa have since enacted similar comprehensive privacy laws and other states are beginning to follow suit.[18]

Moreover, as we write, privacy law finds itself at somewhat of an inflection point. The FIPP-based notice-and-choice regime that has served as the backbone for most privacy laws is being assailed as outdated in an age of pervasive data collection. As two prominent legal scholars have put it, "'notice' often means little more than burying data practices in the fine print of a dense privacy policy, while 'choice' means choosing to use a service with its non-negotiable data practices as a take-it-or-leave-it option."[19]

This global expansion and evolution of information privacy law leads us to the second reason why a student-focused journal of information privacy law is needed: The task of navigating (and updating) all of this law in the face of emerging technologies will fall on the generation of lawyers that is now beginning to enter the profession. Accordingly, to meet this moment, law schools must foster the interest, engagement, creative problem solving, and professional success of students who want to become privacy attorneys.

The SJIPL aims to do exactly that. The Journal will serve as a platform for law students to research, write, and edit papers that examine novel issues in the field of information privacy law. Students who choose to do so will sharpen their legal skills, gain exposure to new areas of privacy law, demonstrate expertise to potential employers, and—we hope—become even more enthusiastic about practicing in this area of law.

Unfortunately, students who want to publish their scholarly writings about information privacy law currently have limited outlets to do so. Most law journals do not accept submissions from students unless the student is a member of the journal's editorial staff. Even when a journal does accept submissions from students, a student writing about privacy law will have to compete with students writing about any number of other topics. And, students submitting to other journals must generally conform to traditional law journal norms regarding article length (15,000-25,000 words), which (as any professor can attest) may dissuade students from pursuing a research topic altogether.

---

15. Children's Online Privacy Protection Act, Pub. L. 105-277, 112 Stat. 2681(1998) (codified at 15 U.S.C. §§ 6501-6506).

16. Federal Trade Commission Act, 15 U.S.C. § 45.

17. *See* CAL. CIV. CODE. §§ 1798.100-199 (West 2022).

18. *See* Anokhy Desai, *U.S. State Privacy Legislation Tracker*, INT'L ASS'N OF PRIVACY PROFS. (Apr. 12, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (outlining side-by-side comparisons of each state privacy law as enacted).

19. *See, e.g.*, Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1794, 1794 (2020).

In stark contrast, the SJIPL will *only* accept submissions from students and *only* when those submissions pertain to information privacy law. Moreover, the SJIPL's e-publication format gives the Journal more flexibility in article length than traditional print publications may enjoy.

Third, and relatedly, we believe students have a valuable voice to add to the conversation around information privacy law. Students can offer a fresh perspective on issues that have become stale to professionals and can unveil issues to which more seasoned generations may be blinded. Moreover, many students choose to pursue a career in privacy law after having gained expertise working in related industries. At Maine Law, for example, current and recent privacy law students have had prior careers in computer science, healthcare, insurance, banking, human resources, military intelligence, journalism, adtech, and more. These students can provide valuable insights where their professional expertise intersects with their studies of information privacy law.

The University of Maine School of Law is the ideal institution to house a student-authored journal dedicated to information privacy law. Maine Law was one of the first schools in the country to begin regularly teaching information privacy law and was the second school to offer a Certificate in Information Privacy Law. The law school hosts the annual Summer Privacy Institute, which draws world-renowned professors and practitioners to teach in Portland for three weeks during the early summers. Maine Law has an active student group on-point, the Maine Law Information Privacy Association. And, Maine Law students regularly complete privacy-related internships and externships with highly regarded organizations across the country. The school's commitment to information privacy law has resulted in an "impressive number of Maine Law graduates working in privacy law for large companies and firms," particularly considering "the law school's small size."[20]

## II. WHAT THE SJIPL PUBLISHES

Here, we describe the three types of writings that the SJIPL currently publishes. We note, too, that the SJIPL's publication structure will likely change with time, as future editorial staffs experiment with new concepts. Indeed, the flexibility to depart from some norms of traditional law journals is a luxury the SJIPL enjoys as a new journal that publishes in electronic format.

The SJIPL publishes monthly editions during the school year. These editions are comprised of two types of writings: Commentary Blog Posts and Papers. Commentary Blog Posts are casual, shorter-form submissions (as blog posts generally are) that offer analysis or opinion about current events related to information privacy law. The SJIPL accepts submissions for Commentary Blog Posts from students at Maine Law and from students at other law schools currently pursuing a J.D. or equivalent degree. The SJIPL's editors give such Posts a light editorial touch, allowing the author's work to (mostly) speak for itself.

20. IAPP, *Privacy and Data Protection in Academia: A Global Guide to Curricula* (Nov. 2021), https://iapp.org/media/pdf/resource_center/privacy_data_protection_in_academia_global_guide_to_curricula.pdf.

The Papers that the SJIPL publishes in its monthly editions are privacy-related papers authored by Maine Law students. The SJIPL publishes these Papers to serve as a repository for longer-form privacy writings completed by students during their time at Maine Law. Published Papers may have originally been written for a class, for an independent writing project, for a writing competition, or to satisfy the Journal's writing requirement for staff members. Papers will typically describe an issue in information privacy law and then advance a novel viewpoint or solution regarding that issue. They are longer and more formal publications than Commentary Blog Posts—some may even be comparable in length to traditional law review articles. Like Commentary Posts, the SJIPL's editors give Papers only a modest editorial touch, allowing Maine Law students to showcase their own work.

Lastly, the SJIPL publishes Articles in its annual paginated editions. Articles are formal publications that explore a legal issue related to privacy law in depth and advance a novel take on that issue. They are longer-form pieces, though they need not be 15,000-25,000 words, as many law journals have traditionally required. Only a handful of Articles will be selected for publication each year. Selection of an Article for publication indicates the editorial team's belief that the submission is of high quality and that it contributes meaningfully to the relevant body of scholarship.

The SJIPL accepts submissions for Articles from students at Maine Law and from students at other law schools currently pursuing a J.D. or equivalent degree. Although the SJIPL did receive submissions from students at other law schools, this inaugural edition is comprised of Articles authored by Maine Law students.[21] The Journal anticipates that future editions will contain a mix of Articles authored by Maine Law students and by students from other law schools.

Volume One of the SJIPL's paginated edition contains four Articles. The lead Article is *The Illinois Biometric Privacy Act: History, Developments, and Adapting Protection for the Future*, by Maggie O'Neil. The Article reviews the development and dangers of biometric identification technologies and takes a deep-dive into Illinois' Biometric Information Privacy Act (BIPA). O'Neil then provides policy recommendations for states considering biometric privacy legislation, focusing especially on the importance of including a private right of action. O'Neil's perspective on state-level privacy legislation is particularly apt, as she is a Maine State Representative as well as a student at Maine Law.

Next, Leaning into CHAOS (Child's Health and Online Safety Act): Revision to FTC's Enforcement of COPPA & New Model Rules for Child Advertising, written by Gabrielle Schwartz, focuses on legal protections for children's online privacy. Schwartz critiques the current children's privacy protection regime (COPPA) and prescribes broader protections relative to targeted advertising and to the collection of children's data.

The third Article is *Revenge Porn: The Result of a Lack of Privacy In An Internet-Based Society*, by Shelbie Mora. The Article examines current "revenge porn" statutes in the United States and analyzes their efficacy from victims'

21. The Journal has previously published some submissions from students at other schools as stand-alone (non-paginated) writings in its monthly editions.

perspectives. Mora then reviews pending legislation and proposes suggestions to improve the current laws with stricter penalties.

The final Article is *Life's Not Fair. Is Life Insurance?*, written by Mark Sayre. Sayre unpacks how life insurers' rapid adoption of artificial intelligence techniques could lead to unintentional discriminations. He then warns that current antidiscrimination laws do not guard against this risk and argues that a patchwork of state-based solutions would be undesirable. Instead, Sayre proposes using professional actuarial standards to create a uniform rule against discriminatory AI practices in life insurance.

***

In sum, as its name suggests, the SJIPL exists for and because of students. It is at once a tool for education, for professional mobility, for intellectual connection, and for the exploration of creative remedies to the risks that new technologies pose to our privacy. Our hope is that this platform will continue to grow and to flourish with time, as its first generation of student editors surely will.