How security and privacy research engages with law and policy: analysis and recommendations

Abstract:

Security and privacy researchers have increasingly engaged with the law and with policymakers, particularly in light of data privacy regulation such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). We believe this is a positive development: Security and privacy researchers can and should bring technical evidence that will impact policy in a positive direction. But to ensure that research has that impact, it is first important to understand the particular ways in which security and privacy researchers are engaging with law and policymakers, including the categories of problems being studied, the prevalence of law-and-policy-oriented research, and the general depth of engagement. The accuracy of legal claims in security and privacy papers is also important. Where the validity of a research project turns on the accuracy of legal analysis (e.g., a project studying the impact of a privacy law, but misunderstanding the legal requirements), the impact of incorrect legal claims is quite clear. But even where legal claims are less central, legal misunderstandings can dampen potential policy impact (e.g., if a paper recommends a change to a legal regime, but misunderstands existing law).

Thus, we engage in a systematic analysis of security and privacy research over the past ten years. We study the 5484 papers published at five security and privacy conferences (S&P, CCS, NDSS, USENIX, and PETS/PoPETs) over a ten-year period (2014-2023), by conducting a deep dive into a subset of papers with legal and policy engagement. We present preliminary findings, some of which we sketch here: A significant, and increasing, fraction of papers engage at least minimally with law and policymakers. Of those papers engaging more deeply, three broad categories of papers predominate: large-scale measurement studies of legal compliance, technical papers facilitating legal compliance, and calls for changes to legal requirements. Contrary to our initial expectations, security and privacy researchers are engaging with more than just GDPR/CCPA; papers extend into, for example, election laws, finance, and healthcare. On a cursory, nonrepresentative look, we also find several misstatements about legal requirements. We conclude with actionable recommendations that we believe will facilitate impactful security and privacy research.

Reading list

1. Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina- Rodriguez, and Serge Egelman. “Won’t Somebody Think of the Children?” Examining COPPA Compliance at Scale. In Proceedings on Privacy Enhancing Technologies (PETS), July 2018.
2. Imane Fouad, Cristiana Santos, Arnaud Legout, and Nataliia Bielova. My cookie is a phoenix: Detection, measurement, and lawfulness of cookie respawning with browser fingerprinting. In Proceedings on Privacy Enhancing Technologies (PETS), July 2022.
3. Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. The privacy policy landscape after the GDPR. In Proceedings on Privacy Enhancing Technologies (PETS), July 2020.

4. Rocky Slavin, Xiaoyin Wang, Mitra Bokaei Hosseini, James Hester, Ram Krishnan, Jaspreet Bhatia, Travis D. Breaux, and Jianwei Niu. 2016. Toward a Framework for Detecting Privacy Policy Violations in Android Application Code. In Proceedings of the 38th International Conference on Software Engineering (Austin, Texas) (ICSE ’16). Association for Computing Machinery, New York, NY, USA, 25–36.
5. Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. 2014. Security Analysis of the Estonian Internet Voting System. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). Association for Computing Machinery, New York, NY, USA, 703–715. https://doi.org/10.1145/2660267.2660315
6. Irene Pollach. 2007. What's wrong with online privacy policies? Commun. ACM 50, 9 (September 2007), 103–108. https://doi.org/10.1145/1284621.1284627
7. Randy Connolly. 2020. Why computing belongs within the social sciences. Commun. ACM 63, 8 (August 2020), 54–59. https://doi.org/10.1145/3383444
8. Rediet Abebe, Solon Barocas, Jon Kleinberg, Karen Levy, Manish Raghavan, and David G. Robinson. 2020. Roles for Computing in Social Change. In FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency. https://doi.org/10.1145/3351095.3372871.
9. Anne Spaa, Abigail Durrant, Chris Elsden, and John Vines. 2019. Understanding the Boundaries between Policymaking and HCI. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 84, 1–15. https://doi.org/10.1145/3290605.3300314
10. Vanessa Thomas, Christian Remy, Mike Hazas, and Oliver Bates. 2017. HCI and Environmental Public Policy: Opportunities for Engagement. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17). Association for Computing Machinery, New York, NY, USA, 6986–6992. https://doi.org/10.1145/3025453.3025579
11. Ross Anderson, Security Engineering, Third Edition (2021)
12. James Grimmelmann, Internet Law: Cases and Problems, Thirteenth Edition (2023), chapters 5 and 7.