PRIVACY PAPERS FOR POLICYMAKERS

2021

FUTURE OF PRIVACY FORUM

This material is based upon work supported by the National Science Foundation under Grant No. 1837413.

FUTURE OF
PRIVACY
FORUM

February 10, 2022

We are pleased to introduce FPF's 12th annual Privacy Papers for Policymakers. Each year we invite privacy scholars and authors to submit scholarship for consideration by a committee of reviewers and judges from the FPF Advisory Board. The selected papers are those judged to contain practical analyses of emerging issues that policymakers in Congress, in federal agencies, at the state level, and internationally will find useful.

This year's winning papers examine a variety of topical privacy issues:

- One paper constructs a typology for courts to understand privacy harms so that violations can be addressed in a meaningful way, and provides an approach to when privacy harm should be considered.
- Another paper proposes a rigorous approach for determining whether human oversight of algorithms helps or hinders government efforts to prevent injustices.
- A third paper discusses the manner in which a requirement of data loyalty can be used as a key policy tool for privacy regulation, and proposes four contexts in which specific rules should supplement a general rule of data loyalty.
- The authors of another paper explore what smartphone platforms' role should be in legal frameworks. They argue for a compromise between direct regulation of platforms and mere self-regulation, arguing that platforms should be required to make official disclosures about their privacy-related policies and practices for their respective ecosystems.
- Another paper compares China's new Personal Information Protection Law (PIPL) with the data protection laws of nine other countries, to help companies that handle personal information comply with the data protection laws in each jurisdiction.
- The sixth winning paper offers insight into individuals' diverse preferences on opt-in and opt-out rights for the collection, use and sharing of data associated with video analytics.

For the sixth year in a row, we are proud to continue highlighting student work by honoring *A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps* (Kollnig, et al.). This winning paper offers insight into whether and to what extent consent is implemented in mobile apps using a representative sample of apps in the Google Play Store. It found that a majority of apps analyzed engaged in third-party tracking without obtaining consent before doing so, resulting in potential violations of EU and UK privacy law.

We thank the scholars, advocates, and Advisory Board members who are engaged with us to explore the future of privacy.

Chris Wolf

Christopher Wolf
Founder and Board President,
FPF Board of Directors

Jules Polonetsky

Jules Polonetsky
CEO

Table of Contents

Awarded Papers

Honorable Mentions

Awarded Student Paper

Student Paper Honorable Mention

Out of respect for copyright law and for ease of reference, this compilation is a digest of the papers selected by the Future of Privacy Forum Advisory Board and does not contain full text. The selected papers in full text are available through the referenced links.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the Future of Privacy Forum.

Privacy Harms

Danielle Keats Citron and Daniel J. Solove

Boston University Law Review, Vol. 102, 2022
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222

Executive Summary

The requirement of harm has significantly impeded the enforcement of privacy law. In most tort and contract cases, plaintiffs must establish that they have suffered harm. Even when legislation does not require it, courts have taken it upon themselves to add a harm element. Harm is also a requirement to establish standing in federal court. In Spokeo v. Robins and TransUnion v. Ramirez, the US Supreme Court ruled that courts can override congressional judgment about cognizable harm and dismiss privacy claims.

Caselaw is an inconsistent, incoherent jumble, with no guiding principles. Countless privacy violations are not remedied or addressed on the grounds that there has been no cognizable harm.

Courts struggle with privacy harms because they often involve future uses of personal data that vary widely. When privacy violations result in negative consequences, the effects are often small — frustration, aggravation, anxiety, inconvenience — and dispersed among a large number of people. When these minor harms are suffered at a vast scale, they produce significant harm to individuals, groups, and society. But these harms do not fit well with existing cramped judicial understandings of harm.

This article makes two central contributions. The first is the construction of a typology for courts to understand harm so that privacy violations can be tackled and remedied in a meaningful way. Privacy harms consist of various different types, which to date have been recognized by courts in inconsistent ways. Our typology of privacy harms elucidates why certain types of privacy harms should be recognized as cognizable.

The second contribution is providing an approach to when privacy harm should be required. In many cases, harm should not be required because it is irrelevant to the purpose of the lawsuit. Currently, much privacy litigation suffers from a misalignment of enforcement goals and remedies. We contend that the law should be guided by the essential question: When and how should privacy regulation be enforced? We offer an approach that aligns enforcement goals with appropriate remedies.

Authors

Danielle Keats Citron is the Jefferson Scholars Schenck Distinguished Professor in Law, Caddell & Chapman Professor of Law at the University of Virginia School of Law where she directs the LawTech Center. She is the Vice President of the Cyber Civil Rights Initiative and a 2019 MacArthur Fellow. She is the author of *Hate Crimes in Cyberspace* (2014) and 50 law review articles and essays. Her book *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* is forthcoming in W.W. Norton and Penguin Vintage UK in the summer 2022.

Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also the founder of TeachPrivacy, a company that provides privacy and data security training programs to businesses, law firms, healthcare institutions, schools, and other organizations. One of the world's leading experts in privacy law, Solove is the author of 10+ books and textbooks and 50+ articles. His most recent book is *Breached!: Why Data Security Law Fails and How To Improve It* (Oxford University Press, March 2022) (with Woodrow Hartzog). His articles have appeared in the Harvard Law Review, Yale Law Journal, Stanford Law Review, and Columbia Law Review, among others. Professor Solove writes at LinkedIn as one of its "thought leaders," and he has more than 1 million followers. He more routinely blogs at Privacy+Security Blog.

The Flaws of Policies Requiring Human Oversight of Government Algorithms

Ben Green

Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3921216

Executive Summary

Policymakers around the world are increasingly considering how to prevent government uses of algorithms from producing injustices. One mechanism that has become a centerpiece of global efforts to regulate government algorithms is to require human oversight of algorithmic decisions. Despite the widespread turn to human oversight, these policies rest on an uninterrogated assumption: that people are able to oversee algorithmic decision-making. This article surveys 40 policies that prescribe human oversight of government algorithms and find that they suffer from two significant flaws. First, evidence suggests that people are unable to perform the desired oversight functions. Second, as a result of the first flaw, human oversight policies legitimize government uses of faulty and controversial algorithms without addressing the fundamental issues with these tools. Thus, rather than protect against the potential harms of algorithmic decision-making in government, human oversight policies provide a false sense of security in adopting algorithms and enable vendors and agencies to shirk accountability for algorithmic harms. In light of these flaws, this article proposes a more stringent approach for determining whether and how to incorporate algorithms into government decision-making. First, policymakers must critically consider whether it is appropriate to use an algorithm at all in a specific context. Second, before deploying an algorithm alongside human oversight, agencies or vendors must conduct preliminary evaluations of whether people can effectively oversee the algorithm.

Author

Ben Green is a Postdoctoral Scholar in the Michigan Society of Fellows and an Assistant Professor in the Gerald R. Ford School of Public Policy. He holds a PhD in Applied Mathematics, with a secondary field in Science, Technology, and Society, from Harvard University. Professor Green studies the social and political impacts of government algorithms, with a focus on algorithmic fairness, human-algorithm interactions, and AI regulation. His book, *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*, was published in 2019 by MIT Press. Professor Green is also an Affiliate at the Berkman Klein Center for Internet & Society at Harvard and a Non-Resident Fellow at the Center for Democracy and Technology.

The Surprising Virtues of Data Loyalty

Woodrow Hartzog and Neil M. Richards

Emory Law Journal, Vol. 71 (forthcoming 2022)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3921799

Executive Summary

Duties of data loyalty implementing ideas from privacy law scholarship are now under serious consideration by lawmakers in the US and Europe, yet critics charge that such duties are unnecessary, unworkable, and indeterminately and fatally vague. This paper takes those criticisms seriously, and its analysis of them reveals that duties of data loyalty have surprising virtues. Loyalty, it turns out, places the focus for information-age problems where it belongs: not just on the data, but on the human relationships that really matter; not just on procedural requirements for data processing, but on substantive rules restricting dangerous applications; and not merely on the interests of individuals, but on the interests of groups with the same relational vulnerabilities. A call for data loyalty can thus become one with meaningful analytical and political consequences. Even loyalty's supposed fatal flaw—its indeterminate vagueness—is a great strength of flexibility and adaptability across contexts, cultures, and time. Simply put, loyalty represents a relational approach to data that allows us to deal substantively with the problem of platforms and human information at the systemic and the individual levels.

The argument in this paper is ultimately a simple one: the concept of data loyalty has surprising virtues, including checking power and limiting systemic abuse. In fact, it may well be the critical piece of the regulatory toolkit for privacy. This paper develops its argument across four parts. First, it argues that one of the main virtues of a duty of loyalty is that it is sensitive to the power imbalances between people and tech companies in ways that existing privacy laws are not. Second, it argues that a duty of loyalty offers substantive protections that a GDPR-style approach does not. Third, it argues that loyalty would serve a broad array of human values in a way that the current lionization of individual choice, consent, and control does not. Finally, it proposes four subsidiary data loyalty duties targeting the four areas most conducive to disloyal and harmful self-dealing by platforms.

Lawmakers should consider creating subsidiary data loyalty rules in four different contexts. First, there is Personalization, the act of treating people differently based upon personal information or characteristics. Second, there is Gatekeeping, the extent to which trusted entities allow third parties to access trusting people and their data. The third context is Influence, where companies leverage technologies to exert sway over people to achieve results. Finally, there is Mediation, which concerns the way that organizations design their platforms to facilitate users interacting with each other. Within these four contexts, the paper explores problems such as discriminatory and harmful microtargeting, design choices that facilitate online harassment, the corrosive amplification of particular behavior, and abusive dark patterns. And it shows how a loyalty perspective can make a difference, not just in how we understand these problems but in how we solve them in practice.

The paper concludes that loyalty, properly understood, should be the foundation of a US data privacy framework. Critics of a duty of loyalty have rightfully pointed out that new legal approaches are required to disrupt the unprecedented power of modern platforms. Lawmakers and scholars have been pushing privacy law towards a particular relational focal point for a while now. It is time we give it a name: loyalty.

Authors

Woodrow Hartzog is a Professor of Law and Computer Science at Northeastern University School of Law and the Khoury College of Computer Sciences. He is also a Faculty Associate at the Berkman Klein Center for Internet & Society at Harvard University, a Non-resident Fellow at the Cordell Institute for Policy in Medicine & Law at Washington University, and an Affiliate Scholar at the Stanford Center for Internet and Society. His research has been published in scholarly publications such as the Yale Law Journal and Columbia Law Review and popular publications such as The New York Times, The Washington Post, and The Guardian. He is the author of Privacy's Blueprint (Harvard Press 2018) and co-author with Daniel Solove of Breached! (Oxford Press 2022).

Neil Richards is the Koch Distinguished Professor in Law at Washington University School of Law, where he co-directs the Cordell Institute for Policy in Medicine & Law. He is also an affiliate scholar with the Stanford Center for Internet and Society and the Yale Information Society Project, and a Fellow at the Center for Democracy and Technology. Professor Richards is the author of Why Privacy Matters (Oxford Press 2021) and Intellectual Privacy (Oxford Press 2015). His many scholarly and popular writings on privacy and civil liberties have appeared in a wide variety of media, from the Harvard Law Review and the Yale Law Journal to The Guardian, WIRED, and Slate.

Smartphone Platforms as Privacy Regulators

Joris van Hoboken and Ronan Ó Fathaigh

Computer Law & Security Review, Vol. 41 (2021)
Available at SSRN: https://doi.org/10.1016/j.clsr.2021.105557

Executive Summary

A series of recent developments highlight the increasingly important role of online platforms in impacting data privacy in today's digital economy. Revelations and parliamentary hearings about privacy violations in Facebook's app and service partner ecosystem, EU Court of Justice judgments on joint responsibility of platforms and platform users, and the rise of smartphone app ecosystems where app behavior is governed by app distribution platforms and operating systems, all show that platform policies can make or break the enjoyment of privacy by users. This article examines these developments and explores the question of what can and should be the role of platforms in protecting data privacy of their users.

The article first distinguishes the different roles that platforms can have in ensuring respect for data privacy in relevant ecosystems. These roles include governing access to data, design of relevant interfaces and privacy mechanisms, setting of legal and technical standards, policing behavior of the platform's (business) users, coordinating responsibility for privacy issues between platform users and the platform, and direct and indirect enforcement of a platform's data privacy standards on relevant players. At a higher level, platforms can also perform a role by translating different international regulatory requirements into platform policies, thereby facilitating compliance of apps in different regulatory environments. And in all of this, platforms are striking a balance between ensuring the respect for data privacy in data-driven environments on the one hand and optimization of the value and business opportunities connected to the platform and underlying data for users of the platform on the other hand.

After this analysis of platforms' roles in protecting privacy, the article turns to the question of what should this role be and how to better integrate platforms in the current legal frameworks for data privacy in Europe and the US. The article will argue for a compromise between direct regulation of platforms and mere self-regulation, in arguing that platforms should be required to make official disclosures about their privacy-related policies and practices for their respective ecosystems. These disclosures should include statements about relevant conditions for access to data and the platform, the platform's standards with respect to privacy and the way in which these standards ensure or facilitate compliance with existing legal frameworks by platform users, and statements with respect to the risks of abuse of different data sources and platform tools and actions taken to prevent or police such abuses. We argue that such integration of platforms in current regulatory frameworks is both feasible and desirable. It would make the role that platforms already have in practice more explicit. This would help to highlight best practices, create more accountability and could save significant regulatory and compliance resources in bringing relevant information together in one place. In addition, it could provide clarity for business users of platforms, who are now sometimes confronted with restrictive decisions by platforms in ways that lack transparency and oversight.

Authors

Joris van Hoboken is a Professor of Law at the Vrije Universiteit Brussels (VUB) and an Associate Professor at the Institute for Information Law (IViR), University of Amsterdam. He works on the intersection of fundamental rights protection (privacy, freedom of expression, non-discrimination) and the regulation of platforms and internet services. At the VUB, he is appointed to the Chair 'Fundamental Rights and Digital Transformation', established at the Interdisciplinary Research Group on Law Science Technology & Society (LSTS), with the support of Microsoft. Previously, Professor Van Hoboken worked at the Information Law Institute (ILI) at New York University Law School, the NYU Stern Center for Business & Human Rights, and CornellTech. In 2008, he was a visiting scholar at the Berkman Klein Center for Internet & Society at Harvard University. Professor van Hoboken obtained his PhD from the University of Amsterdam on the topic of search engines and freedom of expression (2012) and has graduate degrees in Law (2006, University of Amsterdam, cum laude) and Theoretical Mathematics (2002, University of Amsterdam, cum laude). Professor van Hoboken is a regular speaker at international events and conferences and has conducted research for the European Commission, ENISA, UNESCO, the Dutch government and the European Parliament.

Ronan Ó Fathaigh is a Senior Researcher at the Institute for Information Law (IViR), University of Amsterdam, and specializes in fundamental rights, in particular privacy and freedom of expression. He is a member of the Digital Transformation of Decision-Making research initiative at the Amsterdam Law School, examining the normative implications of the shift toward automated decision-making, and the effect on democratic values and fundamental rights. He has published his work in numerous international academic journals, including Communications Law, Journal of Media Law, European Human Rights Law Review, European Data Protection Law Review, Internet Policy Review, and Computer Law & Security Review,and is a regulator contributor to the Strasbourg Observers blog, commenting on current human rights issues. He has a PhD in law from the Human Rights Centre at Ghent University, and is a former legal researcher with the Irish public broadcaster (RTÉ), and former visiting research fellow at Columbia University.

Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions

Jie Wang

Available at SSRN: https://fpf.org/wp-content/uploads/2022/01/Wong_Comparison.pdf

Executive Summary

The Law of the People's Republic of China on the Personal Information Protection Law (the "PIPL") was enacted on August 20, 2021, and officially took effect on November 1, 2021. As the first codified personal information protection law in China, the PIPL draws on and incorporates the legislative experience of advanced overseas regions, as well as the useful contents of the Civil Code, Information Security Technology—Personal Information Security Specification, the Network Security Law, the Electronic Commerce Law, and the Data Security Law, etc., which are related to the PIPL. The PIPL provides comprehensive protection for the rights and interests of personal information subjects in relation to personal information handling, the cross-border transfer of personal information, the obligations of personal information handlers and their compliance obligations, and other specific aspects.

Overall, the introduction of the PIPL officially announces the birth of the cybersecurity and data compliance troika (the Cybersecurity Law, the Data Security Law, and the PIPL) and establishes the rule of law structure and system for personal information protection in China, reflecting China's determination and attitude to attach great importance to the protection and governance of personal information. The purpose of this article is to compare China's PIPL with data protection law of other nine major overseas regions in different dimensions, in order to help overseas Internet companies and personnel that have a lot of contact with personal information to better understand the similarities and differences in data protection in each country/region, as well as the main points of compliance.

Author

Jie Wang is a certified lawyer and the founder of W&W international legal team, Kinding Partners, and is also an expert of UN World Silk Road Forum, and a council member of Information and Communication Law Research Association of Guangdong Province. Ms. Wang holds a Master of International Economic Law and Commercial Law (LL.M) from University of Groningen, the Netherlands, and a bachelor's degree in domestic law. She practices in the field of cyber and internet law, especially Internet products compliance, overseas compliance and global and domestic data protection compliance, and has provided professional legal services to many well-known Internet companies and large and medium-sized foreign enterprises, covering such industry fields as intelligent terminal manufacturing, IOT, Artificial Intelligence, Cloud computing and services, social network platforms, mobile Internet, e-commerce and e-commerce platforms, short video audiovisual live streaming, online games, as well as personal information protection and data security.

Wang has served in Alibaba Entertainment Group and has experience in the cyberlaw field. She is also the founder and the chief executive of the WeChat public account of Overseas Internet Law Watch. She co-authored the "Internet Global Data Compliance Legal Observation Report" and published a number of professional articles in relation to Internet Law and Data Compliance, some of which were published in the Wolters Kluwer Professional Database.

“Did you know this camera tracks your mood?”: Understanding Privacy Expectations and Preferences in the Age of Video Analytics

Shikun Zhang, Yuanyuan Feng, Lujo Bauer, Lorrie Faith Cranor, Anupam Das, and Norman Sadeh

Proceedings on Privacy Enhancing Technologies: April 2021, Pages 282–304
Available at SSRN: https://doi.org/10.2478/popets-2021-0028

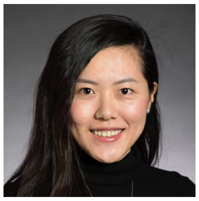
Executive Summary

Cameras are everywhere and increasingly coupled with video analytics software that can identify our faces, record attendance at events, track our moods, and more. The rapid deployment of video analytics across ever more diverse contexts calls for a better understanding of how people feel about these deployments, including their expectations to be notified about and to be able to exercise control over associated data practices. The state of the art today involves notifying data subjects by merely placing signs that read, “this area is under camera surveillance.” This clearly falls short of disclosing a lot of important information and does not provide people with any practical form of control over these data practices, as mandated by regulations such as GDPR or CCPA/CPRA under at least some contexts. The objective of this study is to inform the design of more effective mechanisms to notify people and to give them some control over the collection and use of their data by these technologies. This study also discusses how findings from this work call for new standards and likely also new regulations.

Studying how people feel about video analytics deployments and how to effectively inform them about and give them control over these technologies is challenging for a number of reasons. Failure to adequately capture the many different contextual elements that influence people’s privacy attitudes risks providing a simplistic view of their expectations in this space. This study is the first to capture participants’ responses to a wide range of realistic video analytics deployments in the context of their daily lives over the span of 10 days. In the process, the study gathered a total of 2,328 detailed responses to different video analytics scenarios from 123 participants. These results provide a uniquely rich picture of how people feel towards different deployment scenarios and how their perceptions of these scenarios vary from one individual to another. Overall, while many (though not all) people seem to have grown accustomed to the deployment of some video surveillance technologies, many express surprise and a desire to be informed about and exercise some control over more recent types of deployments such as deployments in the workplace, deployments geared towards marketing or attendance tracking purposes, or video analytics capable of making inferences about someone’s health, including mental health. The study also confirms that people have diverse attitudes towards these different scenarios and that it is essential to have mechanisms that enable them to exercise some control over these practices (e.g., opt-in/opt-out).

The paper discusses the implications of these findings in terms of deploying more effective mechanisms for notice and choice in this space. In particular, its results show that the number of notices that people would receive and privacy choices they might encounter could quickly become unmanageable. The paper advocates for the development of interfaces that simplify the task of managing notices and configuring controls. The development of such interfaces would however require the adoption of standards for notification and for people to communicate their opt-in/opt-out choices to video analytics operators, something that in turn would likely require additional regulation.

Authors



Shikun Zhang is a Ph.D student in the School of Computer Science at Carnegie Mellon University, advised by Professor Norman Sadeh. Her research interests include identifying privacy challenges arising from emerging technologies and exploring usable data-driven approaches to facilitate users' control over their digital privacy. She received her B.S. in Computer Science from Carnegie Mellon University.

Yuanyuan Feng is an Assistant Professor in the Department of Computer Science at the University of Vermont (UVM). Before that, she was a postdoctoral researcher in the School of Computer Science at Carnegie Mellon University (CMU) and earned her Ph.D. in Information Studies from the College of Computing & Informatics at Drexel University. Her research is at the intersection of human-computer interaction (HCI), usable privacy & security, privacy-enhancing technologies, health informatics, ubiquitous computing, and applied machine learning/artificial intelligence (ML/AI). Overall, she investigates both social and technical research topics to ensure the use of people's personal information/data is appropriate, fair, and meaningful.

Lujo Bauer is a Professor of Electrical and Computer Engineering, and of Computer Science, at Carnegie Mellon University. He is also a member of CyLab, Carnegie Mellon's computer security and privacy institute. He received his B.S. in Computer Science from Yale University in 1997 and his Ph.D., also in Computer Science, from Princeton University in 2003. Dr. Bauer's research examines many aspects of computer security and privacy, including developing high-assurance access-control systems, building systems in which usability and security co-exist, and designing practical tools for identifying software vulnerabilities. His recent work focuses on developing tools and guidance to help users stay safer online and on examining how advances in machine learning can (or might not) lead to a more secure future. Dr. Bauer served as the program chair for the flagship computer security conferences of the IEEE (S&P 2015) and the Internet Society (NDSS 2014).

Lorrie Faith Cranor is the Director and Bosch Distinguished Professor in Security and Privacy Technologies of CyLab and the FORE Systems Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University. She is also co-director of the Collaboratory Against Hate: Research and Action Center. She directs the CyLab Usable Privacy and Security Laboratory (CUPS) and co-directs the Privacy Engineering program. In 2016 she served as Chief Technologist at the US Federal Trade Commission. She is also a co-founder of Wombat Security Technologies, Inc, a security awareness training company that was acquired by Proofpoint. She founded the Symposium On Usable Privacy and Security (SOUPS) and co-founded the Conference on Privacy Engineering Practice and Respect (PEPR). She is a fellow of the ACM, IEEE, and AAAS; a member of the ACM SIGCHI Academy; recipient of the 2018 ACM SIGCHI Social Impact Award; and recipient of the 2018 International Association of Privacy Professionals Privacy Leadership Award.

Anupam Das is an Assistant Professor in the Computer Science Department at North Carolina State University (NCSU). Prior to joining the NCSU, he obtained his Ph.D. from the University of Illinois at Urbana-Champaign (UIUC), where he was a recipient of a Fulbright Science and Technology fellowship and also worked as a postdoctoral fellow in the School of Computer Science at Carnegie Mellon University (CMU). His research interests lie in security and privacy, with a special focus on designing secure and privacy-preserving technologies. His current research focuses on exploring the security and privacy challenges in the era of the Internet of Things (IoT), where he focuses on designing systems that can help enhance transparency and control for consumers. He is a recipient of the NSF CRII award (2019). He has also received two ACM Distinguished Paper Awards (ASIACCS 2014, MMSys 2017).

Norman Sadeh is a Professor in the School of Computer Science at Carnegie Mellon University (CMU). He co-founded and co-directs CMU's Privacy Engineering Program and also co-founded and for ten years co-directed CMU's PhD Program in Societal Computing. Until recently, he served as lead principal investigator on two of the largest domestic research projects in privacy, the Usable Privacy Policy project (https://usableprivacy.org) and the Personalized Privacy Assistant Project (https://privacyassistant.org). He also served as founding CEO and, until its acquisition by Proofpoint, as chairman and chief scientist of Wombat Security Technologies. Technologies he developed with colleagues at CMU and Wombat are now used to protect tens of millions of users around the world. In the late nineties he also served as Chief Scientist of the EUR 550 million European Union's e-Commerce initiative, which included all pan-European research in cybersecurity and privacy as well as major related public policy initiatives.

Honorable Mention

Verification Dilemmas and the Promise of Zero-Knowledge Proofs

Kenneth Bamberger, Ran Canetti, Shafi Goldwasser, Rebecca Wexler, and Evan Zimmerman

Berkeley Technology Law Journal: Vol. 37, No. 1, 2022
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3781082

Executive Summary

Individuals who wish to access a website or qualify for a loan are expected to expose personally identifying information undermining privacy and security. Firms share proprietary information in deal-making negotiations which, if the deal fails, may be used by the negotiating partner for a competitive advantage. Regulators are expected to disclose their algorithmic tools to comply with public transparency and oversight requirements, which risks rendering these tools circumventable and ineffective. Litigants might have to reveal trade secrets in court proceedings to prove a claim or defense. Such "verification dilemmas," or costly choices between opportunities that require the verification of some fact and risks of exposing sensitive information in order to perform that verification, appear across the legal landscape. Yet, existing legal responses to them are imperfect. Legal responses often depend on ex post litigation procedures that can be prohibitively expensive for those most in need or otherwise ineffective.

Zero-knowledge proofs (ZKPs)—a class of cryptographic protocols that enables verification of a fact or characteristic of secret information without learning the actual secret—can help avoid these verification dilemmas by providing a feasible means for a party holding secret information to demonstrate desirable properties of this information while keeping the information otherwise secret. Furthermore, ZKPs have recently demonstrated their mettle, for example, by providing privacy backbone to blockchains. Yet they have received scant notice in the legal literature. This Article fills that gap by providing the first deep dive into ZKPs' broad relevance for law. It explains ZKPs' conceptual power and technical operation to a legal audience. It then demonstrates how, and that, ZKPs can be applied as a governance tool to transform verification dilemmas in multiple legal contexts. Finally, the Article surfaces, and provides a framework to address, the policy issues implicated by the potential substitution of ZKP governance tools in place of existing law and practice.

Authors

Kenneth A. Bamberger is The Rosalinde and Arthur Gilbert Foundation Professor of Law at the University of California, Berkeley. He is Faculty co-Director of the Berkeley Center for Law and Technology (BCLT) and of the Berkeley Institute for Jewish Law and Israel Studies, and is a core faculty member of the Berkeley Center for Law and Business (BCLB). Professor Bamberger is an expert on technology, government regulation, and corporate compliance, in both the United States and Europe. At Berkeley, he teaches Administrative Law; the First Amendment (Speech and Religion); Corporate Compliance; Privacy Counseling and Compliance, the Law and Technology Writing Workshop; and Jewish Law. For his recent book, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, Professor Bamberger and his co-author, Berkeley I-School Professor Deirdre Mulligan, were awarded the 2016 Privacy Leadership Award from the International Association of Privacy Professionals. His current work addresses platform market power, consumer expectations and the privacy behavior of free and paid apps, and government use of artificial intelligence and machine learning systems.

Ran Canetti is a Professor of Computer Science in Boston University, where he directs the center for Reliable Information System and Cyber Security. He is a Fellow of the Association for Computing Machinery and the International Association for Cryptologic Research, and an incumbent of the RSA Award in Mathematics. His research interests lie primarily in cryptography and information security, with emphasis on the design, analysis and use of cryptographic algorithms and protocols. Recently he has been studying ways for the co-design of algorithms, law, and policy so as to provide sound foundations for society in the information age.

Shafi Goldwasser is Director of the Simons Institute for the Theory of Computing, and Professor of Electrical Engineering and Computer Science at the University of California Berkeley. Goldwasser is also Professor of Electrical Engineering and Computer Science at MIT and Professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science, Israel. Goldwasser holds a B.S. Applied Mathematics from Carnegie Mellon University (1979), and M.S. (1981) and Ph.D. in Computer Science from the University of California Berkeley (1984).

Professor Goldwasser's pioneering contributions include the introduction of probabilistic encryption, interactive zero knowledge protocols, elliptic curve primality testings, hardness of approximation proofs for combinatorial problems, and combinatorial property testing. She was the recipient of the ACM Turing Award in 2012, the Gödel Prize in 1993 and in 2001, the ACM Grace Murray Hopper Award in 1996, the RSA Award in Mathematics in 1998, the ACM Athena Award for Women in Computer Science in 2008, the Benjamin Franklin Medal in 2010, the IEEE Emanuel R. Piore Award in 2011, the Simons Foundation Investigator Award in 2012, the BBVA Foundation Frontiers of Knowledge Award in 2018, and the L'Oréal-UNESCO For Women in Science Award in 2021. She is a member of the NAS, NAE, AAAS, the Russian Academy of Science, the Israeli Academy of Science, and the London Royal Mathematical Society. Goldwasser holds honorary degrees from Ben Gurion University, Bar Ilan University, Carnegie Mellon University, Haifa University, University of Oxford, and the University of Waterloo, and has received the UC Berkeley Distinguished Alumnus Award and the Barnard College Medal of Distinction.

Rebecca Wexler is an Assistant Professor of Law at the University of California, Berkeley, School of Law, where she teaches, researches, and writes on issues concerning data, technology, and criminal justice. Her work has focused on evidence law, criminal procedure, privacy, and intellectual property protections surrounding new data-driven criminal justice technologies. She is also a Faculty Co-Director of the Berkeley Center for Law & Technology. Professor Wexler's research includes Privacy as Privilege: The Stored Communications Act and Internet Evidence, Harvard Law Review (2021), Privacy Asymmetries: Access to Data in Criminal Defense Investigations, UCLA Law Review (2021), and Life Liberty and Trade Secrets: Intellectual Property in the Criminal Justice System, The Stanford Law Review (2018).

Evan J. Zimmerman is an entrepreneur, investor, and writer. He is the founder of Jovono, through which he invests his money. He is the founder and CEO of Drift Biotechnologies, a company making bioinformatics software. Evan was inducted as the youngest member of the MAK Museum in Vienna's Biennale Circle, which planned the 2017 Vienna Biennale on the "Future Of Work" and was Chairman of the Clinton Health Access Initiative technology council, which advises the technology of global public health in dozens of partner countries. He is a member of the strategy board for Broad Center for Regenerative Medicine at USC. He also speaks and writes on technology, with popular pieces and academic publications in places like Techcrunch, the California Management Review, and the South China Morning Post. He is a cofounder of Mighty Mug and Mighty Ventures, Inc, which has sold millions in 23 countries. Evan has a law degree from Berkeley Law School, where he was a Dean's Scholar with certificates in technology law and business law and won a Prosser award. He graduated from the University of Chicago, where he was a University Scholar, with general and departmental honors in economics and conducted his thesis work on the economics of embargoes as a visiting undergraduate at Harvard University.

Honorable Mention

A Taxonomy of Police Technology's Racial Inequity Problems

Laura M. Moy

University of Illinois Law Review, Vol. 139 (2021)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3340898#

Executive Summary

Over the past several years, increased awareness of racial inequity in policing, combined with increased scrutiny of police technologies, have sparked concerns that new technologies may aggravate inequity in policing. To help address these concerns, some advocates and scholars have proposed requiring police agencies to seek and obtain legislative approval before adopting a new technology, or requiring the completion of "algorithmic impact assessments" to evaluate new tools.

In order for policymakers, police agencies, or scholars to evaluate whether and how particular technologies may aggravate existing inequities, however, the problem must be more clearly defined. Some scholars have explored inequity in depth as it relates to specific police technologies. But to date, none have provided an explanation of how police technology aggravates inequity that can be applied across all technologies—including future technologies we have not yet encountered.

This article fills that gap. It offers a proposed new taxonomy that parses the ways in which police technology may aggravate inequity as five distinct problems: police technology may (1) replicate inequity in policing, (2) mask inequity in policing, (3) transfer inequity from elsewhere to policing, (4) exacerbate inequitable policing harms, and/or (5) compromise oversight of inequity in policing.

Naming and defining these problems will help police agencies, policymakers, and scholars alike analyze proposed new police technologies through an equity lens and craft policies that respond appropriately. This framework should be built into evaluations of police tools performed in accordance with Community Control Over Police Surveillance ("CCOPS") ordinances being passed in a growing number of cities. To assist with these practical applications of the taxonomy, this article also offers a model equity impact assessment for proposed police technologies, and explains why the time is ripe for introduction of such an assessment. Finally, this article explains how the proposed taxonomy and impact assessment tool can be used to evaluate new technologies through an equity lens in contexts beyond the criminal legal system. As policymakers consider requiring algorithmic impact assessments in other domains, they can draw on the framework provided in this article for one possible model.

Author

Laura Moy is an Associate Professor of Law at Georgetown. Professor Moy directs Georgetown's Communications & Technology Law Clinic, where she and a team of staff attorneys and law students represent nonprofit organizations in a range of technology policy matters before agencies and legislative bodies.

Professor Moy has written, spoken, and advocated before agencies and Congress on consumer privacy, algorithmic accountability, law enforcement surveillance, data security, device portability, copyright, and net neutrality. Her current research interests include how technology tools are used in the criminal legal system, and how consumer privacy protections may be leveraged to ensure private information is not used in ways that perpetuate and exacerbate discrimination and other societal ills.

Prior to coming to Georgetown, Professor Moy worked on technology policy issues at New America and Public Knowledge. She completed her B.A. at the University of Maryland, her J.D. at New York University School of Law, and her LL.M. at Georgetown.

Awarded Student Paper

A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps

Konrad Kollnig, Reuben Binns, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt

Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS 2021): August 2021, Pages 181–195
Available at SSRN: https://arxiv.org/abs/2106.09407

Executive Summary

Third-party tracking allows companies to collect users' behavioral data and track their activity across digital devices. This can put deep insights into users' private lives into the hands of strangers, and often happens without users' awareness or explicit consent.

Many privacy laws require consent, both 1) to access and store information on users' devices and 2) to legitimate the processing of personal data as part of third-party tracking. We discuss this in detail for the European Union and United Kingdom in our paper, but also in the US, consent is a cornerstone of privacy law, particularly when it comes to the processing of kids' and health data.

This paper further investigates whether and to what extent consent is implemented in mobile apps:

1. It analyzes a representative sample of apps from the Google Play Store. It finds that most apps engage in third-party tracking (more than 70%), but few (less than 10%) obtain consent before doing so, indicating potentially widespread violations of privacy law.

2. It examines the most common third-party tracking libraries in detail. While most acknowledge that they rely on app developers to obtain consent on their behalf, they typically fail to put in place robust measures to ensure this: disclosure of consent requirements is limited; default consent implementations are lacking; and compliance guidance is difficult to find, hard to read, and poorly maintained.

Author

Konrad Kollnig is a DPhil candidate at the Computer Science Department of Oxford University, with a focus on usable privacy. Previously, he studied computer science and mathematics in Aachen, Edinburgh and Oxford. In his free time, he develops TrackerControl, a privacy app for Android.

Reuben Binns is Associate Professor of Human Centered Computing at the Computer Science Department of Oxford University, working between computer science, law, and philosophy, focusing on data protection, machine learning, and the regulation of and by technology. Between 2018–2020, he was a Postdoctoral Research Fellow in AI at the Information Commissioner's Office, addressing AI / ML and data protection.

Pierre Dewitte is a doctoral researcher at the KU Leuven Centre for IT & IP Law where he conducts interdisciplinary research on privacy engineering, smart cities and algorithmic transparency. His main research track seeks to bridge the gap between software engineering and legal practices to propose a modeling framework that streamlines compliance with Data Protection by Design.

Max Van Kleek is Associate Professor of Human-Computer Interaction in the Computer Science Department of Oxford University. His research area focuses on technologies for human empowerment, at the intersection of human-computer interaction, AI, privacy, IoT, and distributed/web technologies, with a particular recent emphasis on fair, ethical and explainable AI and information architectures.

Ge Wang is a DPhil candidate at the Computer Science Department of Oxford University. Her main research interest is in age-appropriate algorithmic/AI design. She received an MSc in Information Science from University College London in 2018, and a BA in Physics from Oxford University in 2017.

Daniel Omeiza is a DPhil candidate at the Computer Science Department of Oxford University. He joined the University of Oxford after obtaining a bachelor's degree in Computer Science from the University of Ilorin, and a master's degree in Information Technology from Carnegie Mellon University. His research focuses on categorizing explanations and developing post-hoc explanations for autonomous driving.

Helena Webb is Transitional Assistant Professor at the School of Computer Science of Nottingham University. She is an experienced socio-technical researcher with expertise across responsible research and innovation (RRI), human-computer interaction (HCI), science and technology studies, and the sociology of technology. Her research interest lies in the ways in which users interact with technologies in different kinds of settings and how social action both shapes and is shaped by innovation.

Sir Nigel Shadbolt is Professor of Computing Science at the Computer Science Department of Oxford University and Principal of Jesus College, Oxford. In 2012, he co-founded the Open Data Institute, together with Sir Tim Berners-Lee.

Student Paper Honorable Mention

Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent

Yeji Kim
California Law Review (forthcoming February 2022)

Executive Summary

Oculus, a virtual reality company, recently announced that it will require all its users to have a personal Facebook account in order to access its full service. This announcement caused users to fear increased privacy risks from virtual reality, a computer-generated technology that creates a simulated world. The goal of virtual reality is to offer an immersive experience that appears as real as possible to its users. Providing such an experience necessitates collection, processing, and use of extensive user data, which begets corresponding privacy risks. But how extensive are the risks?

This paper examines the unique capacities and purpose of virtual reality and analyzes whether virtual reality data presents fundamentally greater privacy risks than data from other internet-connected devices, such as Internet of Things (IoT), and if so, whether it poses any special challenges to data privacy regulation regimes, namely the European Union's General Data Protection Regulation (GDPR), the world's most stringent and influential data privacy law. Currently, one of the key criticisms of the GDPR is its low and ambiguous standard for obtaining users' "informed consent," or the process by which a fully informed user participates in decisions about their personal data. For example, a user who checks off a simple box after reading a privacy policy gives informed consent under the GDPR.

This paper seeks to contribute to the discussion of the GDPR's regulation of virtual reality data by identifying a more fundamental problem: the futility of text-based informed consent in the context of virtual reality. This paper supports this claim by analyzing how virtual reality widens the gap between the users' understanding of the implications of their consent and the actual implications. It first illustrates how virtual reality service providers must collect and process x-ray-like data from each user, such as physiological data like eye movements and gait, to provide customizations necessary to create an immersive experience. Based on this data, the service providers can know more about each user than what each user knows about themselves. Yet, this knowledge shift is not obvious to users. This is because in order for virtual reality services to provide an immersive experience—a goal unique to virtual reality—customizations based on user data must be unnoticeable to users to avoid distractions. Using Oculus's recent privacy policy as a case study, this Note shows how this hidden knowledge shift transforms the meaning of ordinary privacy policy phrases like "experience unique and relevant to you." What Oculus finds to be "relevant" to the user could be beyond what the user themselves would imagine or notice to be "relevant." As a result, the text becomes an obsolete medium to communicate privacy risks to virtual reality users.

This paper instead proposes other solutions—such as customizable privacy settings and visualization of privacy risks—for users to more closely understand and consciously weigh the benefits and the risks of using virtual reality.

Author

Yeji Kim is a third-year JD candidate at UC Berkeley School of Law. During law school, she has worked with a team at UC Berkeley Law's Samuelson Law & Technology, Public Policy Clinic on issues related to border surveillance and ECPA. She has also spent a summer as a privacy & cybersecurity summer associate in the San Francisco office of Wilson Sonsini Goodrich & Rosati. During law school, she has also externed at the Network Advertising Initiative, helping to draft CPRA comments.

Thank you to our 2021 Reviewers and Finalist Judges

Submissions received numeric rankings from a diverse team of academics, consumer advocates, and industry privacy professionals from the FPF Advisory Board, with each submission being evaluated for originality; overall quality of writing; and applicability to policymaking. For more information, visit fpf.org/privacy-papers-for-policy-makers/.

Advisory Board Reviewers

Daisy Bennett
Instructure, Inc.

Amber Cordova
T-Mobile

Chuck Cosson
T-Mobile US

Scott Cowperthwait
Charter Communications

Rachel Cummings
Columbia University

Carlos Dennis
Samsung Electronics America, Inc.

Sara DePaul
AT&T Services, Inc.

Bill Fusz
Facebook

Laura Gardner
Microsoft

John Gervetz
Visa

Carolina Giuga
The LEGO Group

Anne Klinefelter
University of North Carolina School of Law

Maddie Lamo
ZwillGen Fellow

Barbara Lawler
The Information Accountability Foundation

Professor Yafit Lev-Aretz
Zicklin School of Business, Baruch College, City University of New York

Lucy McGrath
Auth0

Gerome Miklau
Tumult Labs

Douglas Miller
Yahoo

Joan V. O'Hara
XR Association

Carlos Pereira
Willis Towers Watson

Bekah Putz
Chegg Inc.

K Royal
TrustArc

James Spatzek
JPMorgan Chase & Co.

Zoe Strickland
Future of Privacy Forum

Mary Kay Thurlkill, PMP, CIPP/US

Eric Wenger
Cisco Systems

Alexander White
Privacy Commissioner for Bermuda

Ron Whitworth
Truist

Shane Witnov

Scott Uthe
Intel Corporation

Finalist Judges

Agnes Bundy Scanlan, Esq.
President, The Cambridge Group
FPF Board of Directors

Samir Jain
Director of Policy, Center for Democracy & Technology

Jules Polonetsky
CEO, Future of Privacy Forum

John Verdi
Senior Vice President of Policy, Future of Privacy Forum

PRIVACY PAPERS FOR POLICYMAKERS 2021

FUTURE OF PRIVACY FORUM

Future of Privacy Forum (FPF) is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | 202-768-8950