PRIVACY PAPERS FOR POLICYMAKERS

2022

FUTURE OF PRIVACY FORUM

February 16, 2023

We are pleased to introduce FPF's 13th 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 critically elaborates discriminatory practices that African Americans face online, including oversurveillance, exclusion, and predation, and recommends regulation of the digital economy to combat these harms.
- Another paper describes how international privacy and trade law developed together, and proposes a Global Agreement on Privacy.
- Following the fall of *Roe v. Wade,* a third paper proposes placing over-due limits on state surveillance to protect the privacy of personal health data and examines the ability of law enforcement to obtain reproductive health care data.
- Another paper explores the challenges that Data Protection Authorities face in Africa and Latin America, drawing on interviews with regulators and civil society in these regions.
- Another paper describes algorithmic harms and the technical mechanisms that drive those harms, and explores how the FTC's existing authority and new legislation could structurally address these harms.
- The sixth winning paper examines how invasive electronic surveillance deprives people on probation and parole of their fundamental rights.

For the seventh year in a row, we are proud to continue highlighting student work by honoring *Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies.* This winning paper offers insight into regulatory sandboxes, and whether a sandbox instrument should be implemented, with attention to sector-specific concerns.

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

Christopher Wolf
Founder and Board President,
FPF Board of Directors

Jules Polonetsky
CEO

Table of Contents

Awarded Papers

Honorable Mention

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.

Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform

Anita L. Allen

Yale Law Journal, Vol. 131, 2021–2022
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4022653

Executive Summary

African Americans online face three distinguishable but related categories of vulnerability to bias and discrimination that I dub the "Black Opticon": discriminatory oversurveillance, discriminatory exclusion, and discriminatory predation. Escaping the Black Opticon is unlikely without acknowledgement of privacy's unequal distribution and privacy law's outmoded and unduly race-neutral façade. African Americans could benefit from race-conscious efforts to shape a more equitable digital public sphere through improved laws and legal institutions. This Essay critically elaborates the Black Opticon triad and considers whether the Virginia Consumer Data Protection Act (2021), the federal Data Protection Act (2021), and new resources for the Federal Trade Commission proposed in 2021 possibly meet imperatives of a race-conscious African American Online Equity Agenda, specifically designed to help dismantle the Black Opticon. The path forward requires jumping those hurdles, regulating platforms, and indeed all of the digital economy, in the interests of nondiscrimination, antiracism, and antisubordination. Toward escaping the Black Opticon's pernicious gaze, African Americans and their allies will continue the pursuit of viable strategies for justice and equity in the digital economy.

Author

Anita L. Allen is the Henry R. Silverman Professor of Law and Professor of Philosophy from the University of Pennsylvania Carey Law School. A graduate of Harvard Law School with a PhD from the University of Michigan in Philosophy, Allen is internationally renowned as an expert on philosophical dimensions of privacy and data protection law, ethics, bioethics, legal philosophy, women's rights, and diversity in higher education. She was Penn's Vice Provost for Faculty from 2013–2020, and chaired the Provost's Arts Advisory Council. A prolific scholar, Allen is an elected member of the National Academy of Medicine, The American Academy of Arts and Sciences, the American Philosophical Society and the American Law Institute.

Privacy and/or Trade

Anupam Chander and Paul M. Schwartz

University Chicago Law Review, Vol. 90, 2023
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531

Executive Summary

International privacy and trade law developed together but are now engaged in significant conflict. Current efforts to reconcile the two are likely to fail, and the result for globalization favors the largest international companies able to navigate the regulatory thicket. In a landmark finding, this Article shows that more than sixty countries outside the European Union are now evaluating whether foreign countries have privacy laws that are adequate to receive personal data. This core test for deciding on the permissibility of global data exchanges is currently applied in a nonuniform fashion with ominous results for the data flows that power trade today.

The promise of a global internet, with access for all, including companies from the Global South, is increasingly remote. This Article uncovers the forgotten and fateful history of the international regulation of privacy and trade that led to our current crisis and evaluates possible solutions to the current conflict. It proposes a Global Agreement on Privacy that would be enforced within the trade order, but with external data privacy experts developing the treaty's substantive norms.

Authors

Professor Anupam Chander is an expert on the global regulation of new technologies. A graduate of Harvard College and Yale Law School, he clerked for Chief Judge Jon O. Newman of the Second Circuit Court of Appeals and Judge William A. Norris of the Ninth Circuit Court of Appeals. He practiced law in New York and Hong Kong with Cleary, Gottlieb, Steen & Hamilton. He has been a visiting law professor at Yale, the University of Chicago, Stanford, Cornell, and Tsinghua. He previously served as the Director of the California International Law Center and Martin Luther King, Jr. Professor of Law at UC Davis. A member of the American Law Institute, he has also served on the Executive Council of the American Society of International Law, where he co-founded the International Law and Technology Interest Group. The author of The Electronic Silk Road (Yale University Press), he serves as a judge of the Stanford Junior International Faculty Forum. A recipient of Google Research Awards and an Andrew Mellon grant on the topic of surveillance, he has served on ICTSD/World Economic Forum expert groups on the digital economy. He serves as an Adjunct Senior Research Scholar at Columbia University's School of International and Public Policy, a faculty advisor to Georgetown's Institute for Technology Law and Policy, and as a faculty affiliate of Yale's Information Society Project.

Paul Schwartz is a leading international expert on information privacy law. He is the Jefferson E. Peyser Professor at UC Berkeley School of Law and a Director of the Berkeley Center for Law and Technology. Schwartz is the author of many books, including the leading casebook, Information Privacy Law, and the distilled guide, Privacy Law Fundamentals, each with Daniel Solove. Information Privacy Law, now in its sixth edition, is used in courses at more than twenty law schools. Schwartz's over fifty articles have appeared in journals such as the Harvard Law Review, Yale Law Journal, Stanford Law Review, Columbia Law Review, and the University of Chicago Law Review. Fluent in German, he contributes to German legal reviews. Schwartz publishes on a wide array of topics including data analytics, telecommunications surveillance, data security breaches, health care privacy, privacy governance, data mining, financial privacy, European data privacy law, and comparative privacy law.

Reproductive Health Care Data Free or For Sale: Post-Roe Surveillance and the "Three Corners" of Privacy Legislation Needed

Eunice Park

N.Y.U. Review of Law & Social Change, forthcoming Vol. 47.3, 2023
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4321244

Executive Summary

Conditions will be harsher now for women than before Roe v. Wade for one key reason: we live in a surveillance state. While reproductive health care will continue to be a political hot button, one way to manage some of the fallout from *Dobbs v. Jackson Women's Health Organization* is by placing over-due limits on state surveillance to protect the politically uncontroversial expectation of privacy for personal data. Specifically, measures are needed to protect the privacy of health care data, and, in particular, reproductive health care data. Currently, law enforcement can obtain such data not only through failings in existing legislation but also via the ample digital breadcrumbs that fall outside any regulatory construct, including data obtainable for "free" by subpoenas, orders, warrants, and geofence warrants; and data "for sale" by data brokers, including sensitive geolocation information and data from fertility apps.

Author

Eunice Park is Associate Professor of Law at Western State College of Law where she teaches Torts. Professor Park's scholarship explores the tension between digital data and privacy, focusing on topics such as biometrics, smart technology, and AI. Professor Park's article on the third-party data generated by private genomic testing services and smart devices was published in the Yale Journal of Law and Technology, and her article on warrantless cell phone searches, which anticipated Riley v. California, was referenced in the Petition for Writ of Certiorari to the United States Supreme Court. The article described in the Abstract is forthcoming in the N.Y.U. Review of Law and Social Change in summer 2023.

Professor Park completed her B.A. at Smith College and her J.D. at the University of Michigan Law School.

Understanding the Challenges Data Protection Regulators Face: A Global Struggle Towards Implementation, Independence, & Enforcement

Pawel Popiel and Laura Schwartz-Henderson

Available at: https://adapt.internews.org/wp-content/uploads/2022/07/DataProtectionRegulators_July2022_ADAPT.pdf

Executive Summary

With growing diffusion of internet access in the Global South and rapidly expanding and integrating global data economies, Data Protection Authorities (DPAs) have become central actors in governing regional data flows. This report examines the challenges facing DPAs in Africa and Latin America. Drawing on academic and policy literature on implementing and enforcing data protection frameworks in the Global South and interviews with data protection regulators and civil society representatives from Africa and Latin America, this report assesses challenges related to: 1) Establishing a DPA; 2) DPAs' funding and capacity; 3) Independence in structure and decision-making; 4) Compliance and raising awareness; 5) Enforcement; 6) Tackling emerging policy issues; and 7) Collaboration within and across regions with other DPAs and with civil society. The report identifies two prominent factors as key obstacles to effective data protection oversight: resource constraints and threats to independence. The report also identifies essential best practices and recommendations aimed at tackling these challenges. In particular, the interviewees highlighted collaboration between regional DPAs and between DPAs and civil society as especially useful strategies for raising public and private sector awareness, pooling resources, sharing best practices, increasing expertise, and assisting with litigation and enforcement. Moreover, such policy networks can also foster mutual accountability, potentially offsetting or reducing threats to DPA independence. Interviewees also noted that a related priority involves bolstering regional education to facilitate the cultivation of local expertise and community-level awareness of data protection rights and laws. Such expertise and familiarity are essential to effective enforcement, high compliance with data protection regulations, and to making data protection issues as political and social priorities.

Authors

Pawel Popiel is the George Gerbner Postdoctoral Fellow at the University of Pennsylvania's Annenberg School for Communication. Prior to this, he was a postdoctoral fellow at the Media, Inequality, and Change (MIC) Center at Rutgers University and the University of Pennsylvania. His work focuses on the political economy and regulation of digital media and communication technologies. His current research examines the politics and the blurring lines of competition law and policy in media and digital platform sectors. His work has been published in academic journals, edited books, and he has contributed to several policy reports. In 2017, he co-authored the report "The Media Democracy Agenda: The Strategy and Legacy of FCC Commissioner Michael J. Copps" (with Victor Pickard, published by the Benton Foundation), and "Digital Propaganda or 'Normal' Political Polarization? Case study of political debate on Polish Twitter" (published by the Panoptykon Foundation). He received a Ph.D. from the University of Pennsylvania.

Laura Schwartz-Henderson works as the Research & Advocacy Advisor on Internews' Global Technology team, where she develops research, programs, and campaigns on technology policy in diverse political contexts around the world. In this work, she manages programs on data protection, surveillance, content moderation, access, and disinformation. Her research has focused on assessing advocacy capacity for engaging on complex technical issues and on how donor organizations and philanthropies can more strategically support tech policy innovation. Laura was previously the Research Project Manager at the Internet Policy Observatory at the University of Pennsylvania where she managed programs to build methodological literacy and incentivize collaboration between academics working on digital issues, policymakers, and practitioners. She is the founder of the Creative Digital Rights Advocacy Collab Network and the Executive Producer of the Privacy is Global podcast.

Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission

Rebecca Kelly Slaughter; with Janice Kopec and Mohamad Batal

Yale Journal of Law & Technology, Vol. 23, Special Issue 1
Available at: https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf

Executive Summary

This article offers three primary contributions to the existing literature. First, it provides a baseline taxonomy of algorithmic harms that portend injustice, describing both the harms themselves and the technical mechanisms that drive those harms. Second, it describes my view of how the FTC's existing tools—including section 5 of the FTC Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, and market studies under section 6(b) of the FTC Act—can and should be aggressively applied to thwart injustice. And finally, it explores how new legislation or an FTC rulemaking under section 18 of the FTC Act could help structurally address the harms generated by algorithmic decision-making.

Authors

Rebecca Kelly Slaughter was sworn in as a Federal Trade Commissioner on May 2, 2018.

Commissioner Slaughter brings to the Commission more than a decade of experience in competition, privacy, and consumer protection. She builds consensus for a progressive vision, and staunchly advocates for our nation's consumers and workers. Commissioner Slaughter believes that the FTC's dual missions of promoting competition and protecting consumers are interconnected and complementary, and she is mindful that enforcement or rulemaking in one arena can have far-reaching implications for the other.

A proponent of greater resources, transparency, and comprehensive use of the FTC's authorities, Commissioner Slaughter is outspoken about the growing threats to competition and the broad abuse of consumers' data. Targeted merger retrospectives, corrective enforcement, and expansion of the Commission's rulemaking authorities are among the approaches that she has championed during her time at the FTC. Along with advocating for consumers, particularly those traditionally underrepresented and marginalized, Commissioner Slaughter strongly supports working families and work-life balance.

Before joining the FTC, Ms. Slaughter served as Chief Counsel to Senator Charles Schumer of New York, the Democratic Leader. She was an associate in the D.C. office of Sidley Austin LLP before entering federal service.

Ms. Slaughter received her B.A. in Anthropology magna cum laude from Yale University and her J.D. from Yale Law School, where she served as an editor on the Yale Law Journal. She lives in Maryland with her wonderful husband and their four amazing children.

Janice Kopec is the Assistant Director of the Federal Trade Commission's Division of Advertising Practices. She supervises investigations, enforcement actions and rulemaking initiatives relating to unfair and deceptive advertising practices. Previously at the FTC, Janice served as a consumer protection advisor to Commissioners Rebecca Kelly Slaughter and Terrell McSweeny and as an attorney in the Bureau of Consumer Protection's Division of Marketing Practices. She is a graduate of the College of the Holy Cross and Washington & Lee University School of Law and a parent to two very talkative children, neither of whom adequately guard their privacy.

Mohamad Batal is a first-year Lebanese-American student at Yale Law School. There, he serves as an Editor of the Yale Journal on Regulation, a 1L Representative for the Muslim Law Students' Association, and a volunteer through the International Refugee Assistance Project. He recently joined Yale's Tech Accountability & Competition Project, a newly founded clinic in which law students write briefs, file administrative and legal complaints, draft legislation, and represent clients affected by technology and digital platforms. Under faculty supervision, students often collaborate with policymakers and nationally recognized plaintiff-side firms to help vindicate the rights, and dignity, of vulnerable and disadvantaged groups. Ultimately, Mohamad hopes to draw on his clinic work to pursue a career in public-interest technology law.

Before law school, Mohamad spent four years as an Honors Paralegal at the Federal Trade Commission, first in the Bureau of Consumer Protection and then in the Office of Commissioner Slaughter. In both roles, he was fortunate to have a wealth of passionate and brilliant mentors who inspired him to pursue a legal career in public service.

Mohamad received his B.A. at Claremont McKenna College, where he graduated magna cum laude with majors in Government and Philosophy, Politics & Economics. As an undergraduate, Mohamad was the co-founder and president of CMC's Middle Eastern and North African Culture Club and was awarded Best Thesis (2018) by the Government Department. He is an avid Liverpool F.C. fan and enjoys choral music, live theater, and practicing mindfulness.

Punitive Surveillance

Kate Weisburd

Virginia Law Review, Vol. 108, Issue 1, 2022
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3808657

Executive Summary

Budget constraints, bipartisan desire to address mass incarceration, and the COVID-19 crisis in prisons have triggered state and federal officials to seek alternatives to incarceration. As a result, invasive electronic surveillance—such as GPS-equipped ankle monitors, smart phone tracking, and suspicionless searches of electronic devices—is often touted as a humane substitute for incarceration. This type of monitoring, which I term "punitive surveillance," allows government officials, law enforcement and for-profit companies to track, record, share and analyze the location, biometric data and other meta-data of thousands of people on probation and parole. With virtually no legal oversight or restraint, punitive surveillance deprives people of fundamental rights, including privacy, speech, and liberty.

Building on the critique that this type of surveillance is a form of racialized carceral control, this Article makes three contributions: First, drawing on original empirical research of almost 250 public agency records governing the operation of electronic ankle monitoring, this Article reveals non-obvious ways that punitive surveillance, like incarceration, strips people of basic rights and liberties. In particular, the records show how electronic monitoring restricts movement, limits privacy, undermines family and social relationships, jeopardizes financial security and results in repeated loss of freedom. Second, this Article explains how, and why, courts' labeling of such surveillance as a "condition" of punishment or a regulatory measure stems from a misunderstanding of this surveillance technology and punishment jurisprudence. Third, this Article examines whether a fundamental rights analysis, a regulatory response or an abolitionist approach is the most effective way of limiting—if not outright eliminating—punitive surveillance.

Author

Kate Weisburd's primary interests are in the areas of criminal investigation, adjudication, post-conviction law, and civil rights. Professor Weisburd's research focuses on alternatives to incarceration, including the emerging and varied forms of electronic surveillance and non-carceral punishments. Her recent scholarly work has appeared or is forthcoming in the California Law Review, Virginia Law Review, Iowa Law Review, North Carolina Law Review, and the UCLA Law Review, and she has written for The Marshall Project, as well as other mainstream media. Professor Weisburd's article, "Punitive Surveillance" (Va. L. Rev.), was selected for the Reidenberg-Kerr Award for Outstanding Scholarship by a Junior Scholar at the 2021 Privacy Law Scholars Conference.

Prior to joining GW Law, she founded and directed the Youth Defender Clinic at the East Bay Community Law Center, which is part of the clinical program at UC Berkeley School of Law and the largest provider of free legal services in the county. In that role, Professor Weisburd taught and supervised law students representing young people in juvenile court and school discipline proceedings. In addition to her clinical teaching responsibilities, Professor Weisburd served as a lecturer at Berkeley Law, teaching courses on the school-to-prison pipeline. Prior to creating the Youth Defender Clinic, she was a fellow and supervising attorney in Berkeley Law's Death Penalty Clinic. In both clinics, Professor Weisburd maintained her own caseload and represented clients at trial, on appeal, and in post-conviction proceedings.

Professor Weisburd graduated from Columbia Law School, where she received the Bernstein Litowitz Berger & Grossmann Fellowship for Public Interest and the Public Interest Peer-of-the-Year award. Prior to attending law school, she worked as an investigator in death penalty cases at the Southern Center for Human Rights in Atlanta, Georgia. Professor Weisburd received her BA from Brown University, where she was a Truman Scholar. She clerked for the Honorable Lawrence K. Karlton in the U.S. District Court for the Eastern District of California.

Honorable Mention

The art of data privacy

Claire McKay Bowen

Royal Statistical Society Significance, Vol. 19, Issue 1, 2022, Pages 14–19
An excerpt from: Protecting Your Privacy in a Data-Driven World
Available at: https://doi.org/10.1111/1740-9713.01608

Executive Summary

At what point does the sacrifice to our personal information outweigh the public good? If public policymakers had access to our personal and confidential data, they could make more evidence-based, data-informed decisions that could accelerate economic recovery and improve COVID-19 vaccine distribution. However, access to personal data comes at a steep privacy cost for contributors, especially underrepresented groups.

"The art of data privacy" is an excerpt from the book, Protecting Your Privacy in a Data-Driven World, by Claire McKay Bowen, that explains the importance of balancing these competing needs and calls for careful consideration of how data is collected and disseminated by our government and the private sector. Not addressing these concerns can harm the same communities the policymakers are trying to protect through data privacy and confidentiality legislation.

Author

Claire McKay Bowen (she/her) is a principal research associate in the Center on Labor, Human Services, and Population and leads the Statistical Methods Group at the Urban Institute. Her research focuses on developing and assessing the quality of data privacy and confidentiality methods and improving science communication. In 2021, the Committee of Presidents of Statistical Societies identified her as an emerging leader in statistics for her technical contributions and leadership to statistics and the field of data privacy and confidentiality. She is also a member of the Census Scientific Advisory Committee, a committee member of the National Academies of Sciences, Engineering, and Medicine Approaches for Data Governance and Protecting Privacy, an advisory board member of the Future of Privacy Forum, and an adjunct professor at Stonehill College.

Bowen holds a Honors BS in mathematics and physics from Idaho State University and an MS and PhD in statistics from the University of Notre Dame. After completing her PhD, she worked at Los Alamos National Laboratory, where she investigated cosmic ray effects on supercomputers.

Awarded Student Paper

Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies

Walter G. Johnson

Regulation and Governance, 2022
Available at: https://onlinelibrary.wiley.com/doi/10.1111/rego.12487

Executive Summary

Regulatory sandboxes have become the latest development in regulatory reform, starting first in financial regulation and now expanding to other sectors. While sandboxes offer notable potential benefits for managing emerging technologies, achieving desirable policy outcomes with this novel regulatory instrument also comes with technical and political challenges. This article offers a framework to characterize regulatory sandboxes in any sector, involving a blend of (1) approval regulation with broad-based standards, (2) restricted discretion by the regulator for specific norms, (3) process-oriented regulation, (4) an outcomes-orientation, and (5) structured regulator–regulatee information sharing or dialogue. Using this model, the article outlines issues in compliance and legitimacy, including in trust and accountability, responsive enforcement, the politics of participation, and post-sandbox oversight. The article concludes by calling for greater scrutiny when considering implementing a sandbox instrument, with attention to sector-specific concerns, and offering directions for empirical evaluation of regulatory sandboxes.

Author

Walter G. Johnson joined RegNet in 2021 to investigate how regulatory systems are shaping, and being shaped by, emerging neurotechnologies. Walter's research examines the ethical, social, and legal dimensions of a variety of current and emerging technologies with the overarching goal of promoting health, safety, and equity. His work has covered topics from heritable human genome editing to quantum computing.

Before commencing PhD studies at RegNet, Walter was a research fellow for Associate Dean Diana Bowman at the Sandra Day O'Connor College of Law at Arizona State University, where he conducted research on governance for mitochondrial donation and smart cities. He holds a Juris Doctor (JD), Master's in science policy, and a Bachelor's degree in chemistry from Arizona State University.

Student Paper Honorable Mention

My Cookie is a phoenix: detection, measurement, and lawfulness of cookie respawning with browser fingerprinting

Nataliia Bielova, Imane Fouad, Arnaud Legout and Cristiana Santos

Proceedings on Privacy Enhancing Technologies, Vol. 2022, Pages 79–98
Available at: https://petsymposium.org/popets/2022/popets-2022-0063.pdf

Executive Summary

This work presents a large scale study of cookie respawning with browser fingerprinting, a tracking technique that is devoid of a clear legal interpretation in the EU legal framework. We study how trackers can benefit from the combination of the both stateful and stateless web tracking techniques, which have been so far always measured separately. To benefit from both techniques, the tracker can first use a browser fingerprint to create an identifier and store it in the browser's cookie. In this way, even if a user cleans this cookie, the identifier can be recreated with a browser fingerprint. Moreover, even if the fingerprint changes over time, the identifier stored in the cookie can help to match the new fingerprint with the old fingerprint of the same user. Such technique can ensure a persistent, and stable tracking. To the best of our knowledge, our study is the first to detect and measure cookie respawning via browser and machine fingerprint. Our results showed that over 3.8% of the top 30k Alexa websites deployed this tracking mechanism.

This paper was the first to assess the legal consequences of this practice and provides recommendations to policymakers. We show that cookie respawning with browser and machine fingerprint lacks legal interpretation and merits attention for its plausible legal consequences, since in practice, it violates the GDPR and the ePrivacy Directive, not only from the consent perspective, but also from the core principles of data protection (fairness, transparency and law fulness principles).

Respawning seems to be inconsistent with the user's expectations regarding respawned cookies after its deletion from their browser, therefore we consider that all 1,425 respawned cookies violates the fairness principle. Moreover, we analyzed the top 10 respawned cookie owners, and we found that some policies refer to the use of browser's features without referencing the consequences or risks thereof. Also, none of the policies refer to cookie respawning. As such, these seem to be in breach of the transparency principle. Finally, we evaluated whether respawned cookies are subject to or exempted from the legal basis of consent. We found that out of 336 respawned cookies categorized by Cookiepedia, 130 (38.69%) are subject to consent. Hence, these 130 cookies are in breach of the lawfulness principle. We additionally detected that 21 cookies are respawned in sensitive websites without explicit consent to legitimize such operation, rendering such respawning practise unlawful. In the paper we provide proactive suggestions to policymakers with regard to the studied core GDPR principles: fairness, transparency, and lawfulness.

Despite the intrusiveness of this practice, it has been overlooked in the EU Data Protection Law and it is not researched in legal scholarship, nor audited by supervisory authorities. However, owners of respawned cookies and website owners that embed those may be jointly responsible for their usage and may then be subject to fines of up to 20 million EUR or 4% of the total worldwide annual turnover of the preceding financial year. We believe this work can serve as a foundation for improvement of future regulation and protection mechanisms.

Authors

Nataliia Bielova is a Tenured Research Scientist at the French National Institute for Research in Digital Science and Technology (Inria) since 2013. She is a privacy expert with a multidisciplinary background in computer science and law, and investigating privacy and data protection on the Web. She is the recipient of a Young Researcher Award from the French National Research Agency (ANR) in 2018, Inria Doctoral Supervision and Research award in 2017 and 2021, and Best of ACM CHI Honorable Mention award in 2021. During 2021–2022, she was a Senior Privacy Fellow at the French Data Protection Authority (CNIL).

Imane Fouad is currently a Postdoctoral Researcher at Univ. Lille, CNRS, Inria. Fouad is working in the Spirals team on detection and measurement of web tracking. Before, Fouad did her PhD at INRIA Sophia Antipolis with the PRIVATICS team on the same topic under the supervision of Nataliia Bielova and Arnaud Legout. Fouad's main research interest is Privacy protection, Web Tracking technologies, and Legal compliance.

Cristiana Santos is an Assistant Professor in Privacy and Data Protection Law, holding a permanent position at Universiteit Utrecht. Santos holds a joint international Doctoral Degree in Law, Science and Technology (University of Bologna) and a Ph.D. Degree in Computer Science (University of Luxembourg). Santos's PhD thesis focused on modeling relevant legal information using computational ontologies. Currently, Santos is an expert of the Data Protection Unit, Council of Europe; expert for the implementation of the EDPB's Support Pool of Experts; and expert of the Digital Persuasion or Manipulation Expert Group. Santos was also invited as an external expert evaluator of EU funded proposals. Santos collaborates closely with computer scientists from the PRIVATICS team on online privacy. Previously, Santos was a postdoc at INRIA. Prior to joining academia, Santos was a lawyer and worked as a legal adviser and lecturer at the Portuguese Consumer Protection Organization-DECO.

Arnaud Legout is a senior research scientist at Inria Sophia Antipolis, France, in the project-team DIANA. Legout made two academic breaks, one from 2000 to 2004 to join the startup Castify Networks as an Architect and then CTO assistant, and another one from 2016 to 2020 to found and be the CEO of the startup ElectroSmart.

Legout received his Ph.D. in Communication Systems in 2000 and by HDR (Habilitation à Diriger des Recherches) in 2012. Legout did his thesis work at the Institut Eurecom, France, in the Ernst Biersack's working on Multicast Congestion Control. Legout also received a master degree in mathematics (maîtrise de mathématiques) for the Université de Nice-Sophia Antipolis, France.

Notes

Notes

Thank you to our 2022 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
Privacy Officer
Instructure, Inc.

Aparna Bhushan

Louise Bucolo
Foundation Medicine, Inc.

Christoper Chew
IAPP Asia Advisory Board Member

Chuck Cosson
T-Mobile

Ulrika Dellrud

Jennifer Grace
Counsel, Privacy
Airbnb

Marla Greenberg
Director, Privacy Compliance
Capital One

PJ Hoffman
Amazon

Ariel Fox Johnson
Zoom

Matt Lawless
Truist

Brenda K. Leong

Megan McCollum
Salesforce

Douglas Miller
Amazon

Amanda Presutti
Senior Privacy Manager
Airbnb

Jessica Rich
Kelley Drye & Warren

Javier Salido
Airbnb

Alex Schneider
Kelley Drye & Warren LLP

Gerald Smith
Chief Privacy Officer
Cuebiq

Michael T. Spadea
Senior Managing Director
PwC

Scott Sumner
Dassault Systèmes

Ashley Tan
Vice President
Privacy Paramount Global

Rachel Thompson
Mastercard

Mary Kay Thurlkill, PMP, CIPP/US, CIPM, FIP
Director at AT&T

Linda Trickey

Catherine Tucker
MIT

Ron Whitworth
Truist

Jaclyn Wishnia
BigID

Yafit Lev-Aretz
City University of New York

Cobun Zweifel-Keegan
Managing Director
Washington, D.C., IAPP

Finalist Judges

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

Gabriela Zanfir-Fortuna
Vice President for Global Privacy, Future of Privacy Forum

PRIVACY PAPERS FOR POLICYMAKERS 2022

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 | 202-220-8062