PRIVACY LAW

SCHOLARS CONFERENCE

2022

Conference Brochure & Information

TABLE OF CONTENTS

4 MESSAGE FROM THE CHAIR

5 ABOUT THE CONFERENCE

6 MEET THE TEAM

7 THANK YOU TO OUR SPONSORS

8 PLSC AREA MAP

10 MAP OF PLSC

12 COVID-19 POLICY

13 CONTACT INFORMATION

14 CONFERENCE PROGRAM, DAY ONE

26 CONFERENCE PROGRAM, DAY TWO

2022

PLSC

2022

ARI EZRA WALDMAN

PROFESSOR OF LAW & COMPUTER SCIENCE

Northeastern University

Professor Ari Ezra Waldman, a leading authority on law, technology and society, is a professor of law and computer science at Northeastern University. He directs the School of Law's Center for Law, Information and Creativity (CLIC). Professor Waldman studies how law and technology effect marginalized populations, with particular focus on privacy, misinformation and the LGBT community.

MESSAGE FROM THE CHAIR

Welcome to our first in-person PLSC in two years. This is my eighth PLSC, and my second as chair. Like many of you, I've learned a lot, found friends and mentors, mentors who have become friends, and friends who have become lifelines during these last two years. We can survive difficult and uncertain times in solidarity with each other. I hope this in-person conference, with its strong Covid protocols, will be fulfilling and memorable for all the right reasons.

Over the last year, PLSC has been busy. We've kept what has made PLSC extraordinary--constructive feedback, supportive commentators, and opportunities for professional growth--and adapted PLSC to meet the moment in which we find ourselves. Many of our papers focus on the impacts of data extraction on marginalized communities. Our community has grown to include many more scholars from groups traditionally underrepresented at PLSC. We were able to make PLSC free for all students, PhD candidates, Post Docs, and other early career scholars. And we have support structures in place to guard against harassment and discrimination of any kind. PLSC should be a welcoming place for all, and it's been my mission to make that a reality.

I want to thank the program committee for its hard work, Woody Hartzog and Christo Wilson for rolling out Northeastern's red carpet, Nasser Eledroos for going above and beyond to make the conference function, our many student volunteers, the Northeastern event staff, and, of course, all of you. You are the lifeblood of PLSC and I'm so happy to back with you this year.

ARI EZRA WALDMAN
CHAIR, 2022 PRIVACY LAW
SCHOLARS CONFERENCE

ABOUT THE CONFERENCE

PLSC is the oldest and largest gathering of privacy scholars, researchers, and practitioners in the world. We incubate and critique scholarship at the vanguard of the field of law and technology.

Since 2008, PLSC has assembled a wide array of privacy law scholars and practitioners from around the world to discuss current issues in information privacy law and policy. PLSC is a paper workshop conference. It offers no opportunity or obligation to publish. The goal is to provide support for in-progress scholarship related to information privacy law. To do so, PLSC assembles a wide array of privacy law scholars and practitioners who engage in scholarship. Scholars from non-law disciplines—including but not limited to surveillance studies, technology studies, feminist and queer studies, information studies, critical race studies, social sciences, humanities, and computer science—are critical participants in this interdisciplinary field.

We follow a format in which a discussant, rather than the author, introduces and leads a discussion on a paper. There are no panels or talking heads; attendees read papers in advance and offer constructive feedback as full participants in the workshop. Having your paper accepted is NOT a requirement for attending and contributing to the conference, and indeed many attendees do not present a paper.

The boundaries of privacy as a discipline are dynamic and contested. As such, we take a broad view. Although PLSC emphasizes the law of privacy, concepts from other fields play critical roles in our understanding of privacy and in shaping the law.

MEET THE TEAM

Putting together a hybrid convening after so many years is a team effort.

WOODY HARTZOG
Host

CHRISTO WILSON
Host

NASSER ELEDROOS
Conference Manager

CHELSEA SMITH
Events Manager

DOMINIQUE OREFICE
Events Coordinator

THANK YOU TO OUR SPONSORS

PLSC would not have been possible without the many sponsors who continue to believe in the importance of this convening.

GEORGETOWN LAW
Center on Privacy & Technology

COVINGTON
COVINGTON & BURLING LLP

Washington University in St. Louis
The Cordell Institute

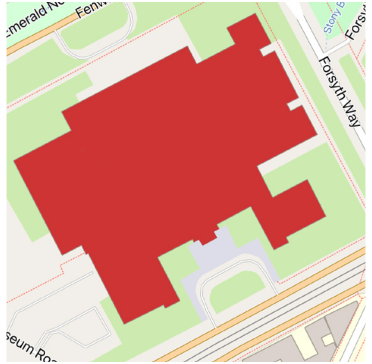
Microsoft

AT&T

iapp

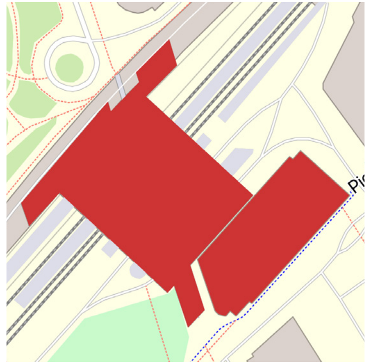
Northeastern University
School of Law
Center for Law, Information and Creativity

PLSC AREA MAP



Museum of Fine Arts, Boston
465 Huntington Ave, Boston

On the evening of June 2nd, the reception for the 2022 Privacy Law Scholars Conference will take place within the Museum of Fine Arts, Boston, conveniently located on Huntington Avenue, a short walk from ISEC on Northeastern's Campus.



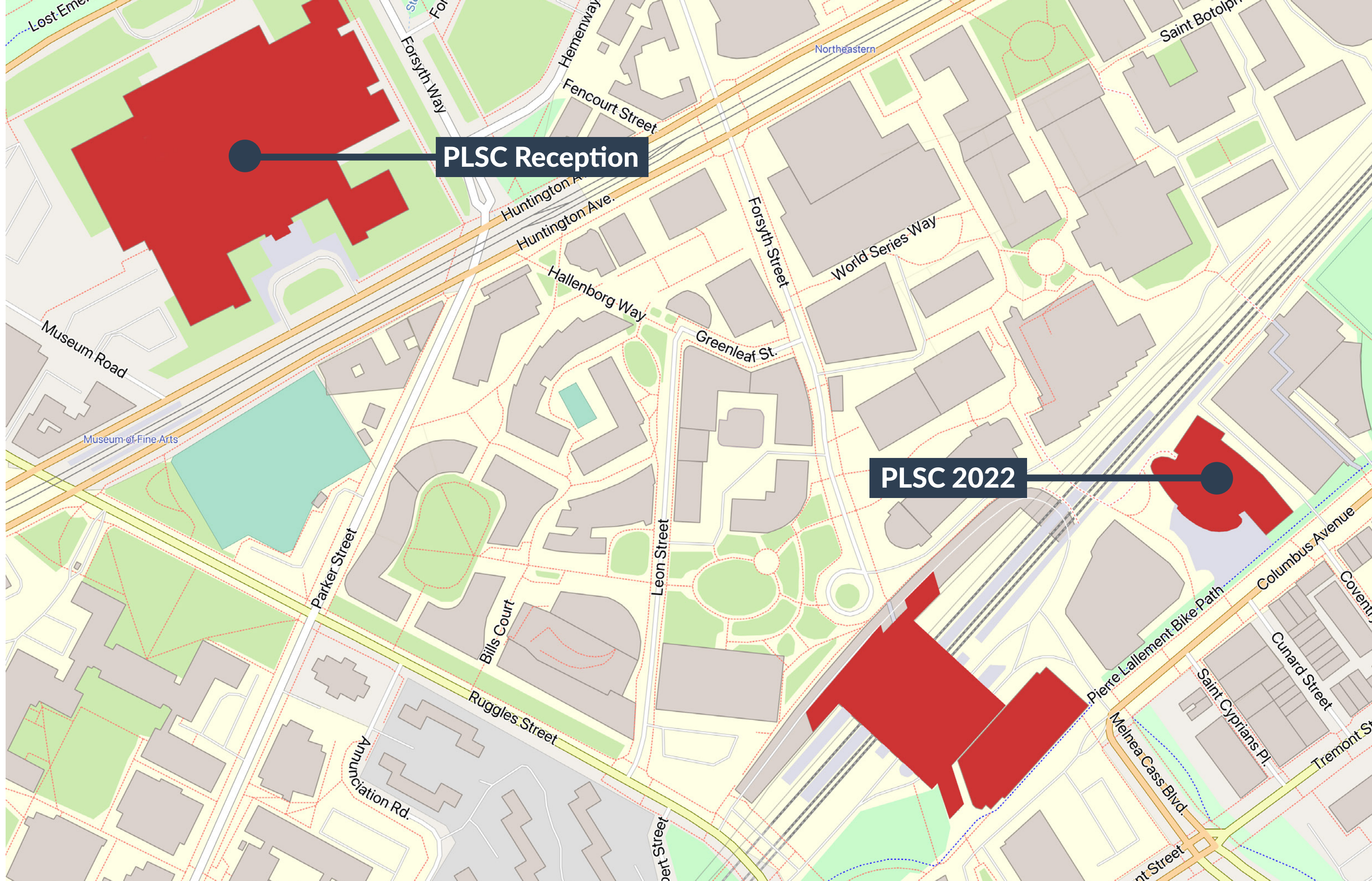
Ruggles MBTA Station
1150 Tremont St, Boston

Conveniently located on campus, Ruggles MBTA station serves the Orange Line subway as well as bus and regional commuter rail.

Bike Path
Columbus Avenue
Covent

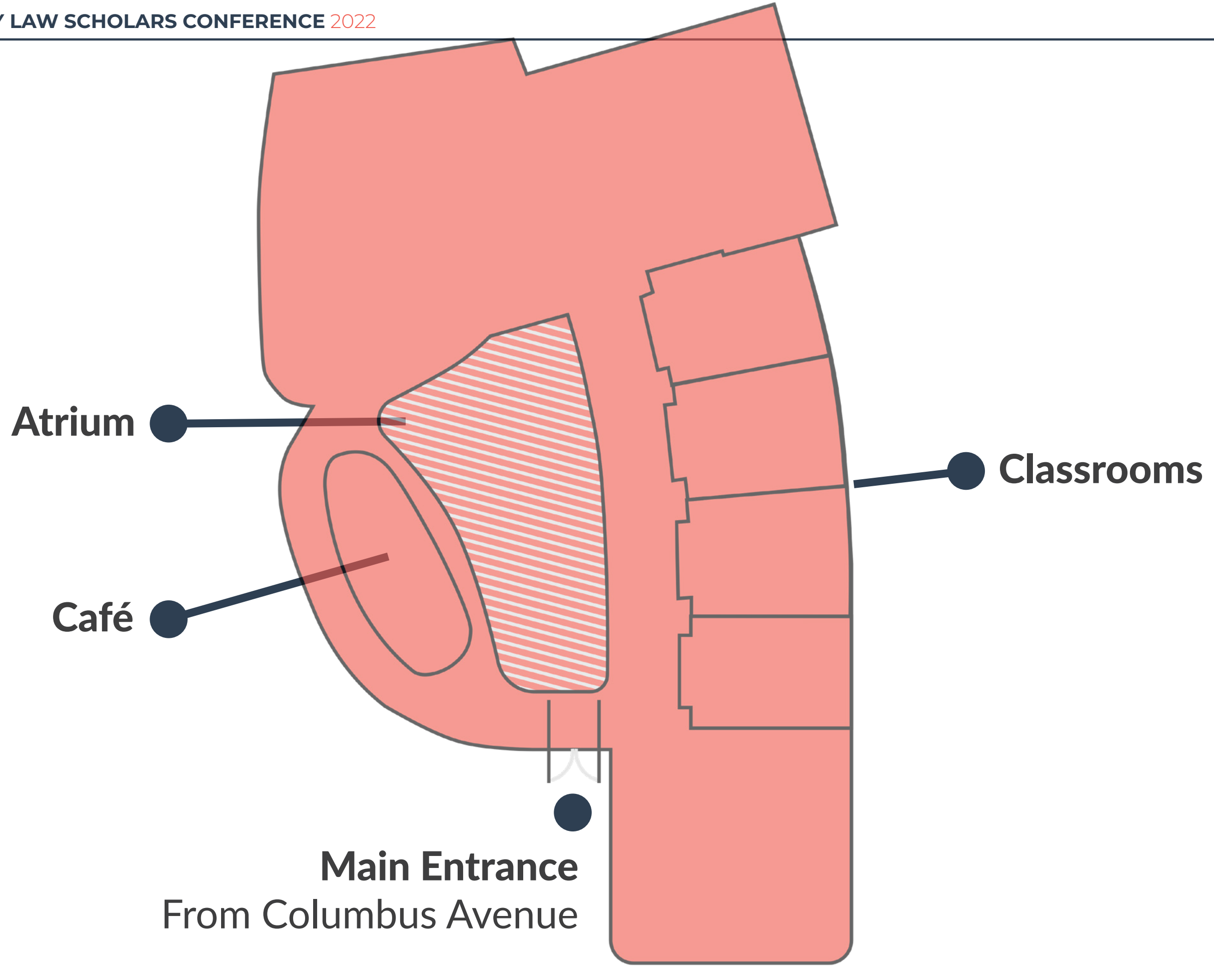
Northeastern "ISEC"
805 Columbus Ave, Boston

Short for "Interdisciplinary Science and Engineering Complex," ISEC is situated a block from Ruggles MBTA Station and is where PLSC will be taking place on June 2nd and 3rd.



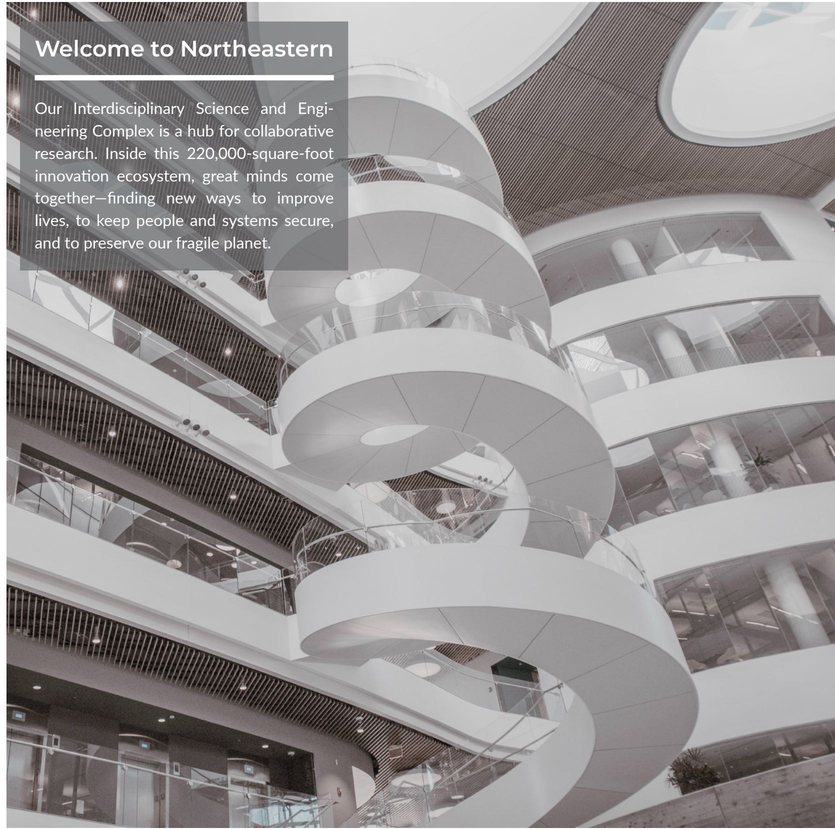
MAP OF PLSC

PLSC takes place within the cavernous Interdisciplinary Science and Engineering Complex (ISEC) at Northeastern University.



PLSC is taking place within several floors inside Northeastern's Interdisciplinary Science and Engineering Complex (ISEC). The map on the left details the ground floor, which is where most of PLSC will take place.

Rooms 432, 532, 632, 655 and 660 are accessible via the elevators.



Welcome to Northeastern

Our Interdisciplinary Science and Engineering Complex is a hub for collaborative research. Inside this 220,000-square-foot innovation ecosystem, great minds come together—finding new ways to improve lives, to keep people and systems secure, and to preserve our fragile planet.

COVID-19 PROTOCOL

To minimize the COVID-19 risk, we are adopting the following protocols for PLSC:

All in-person participants will be required to present proof of vaccination plus at least a single booster upon arrival. (Photographs are fine).

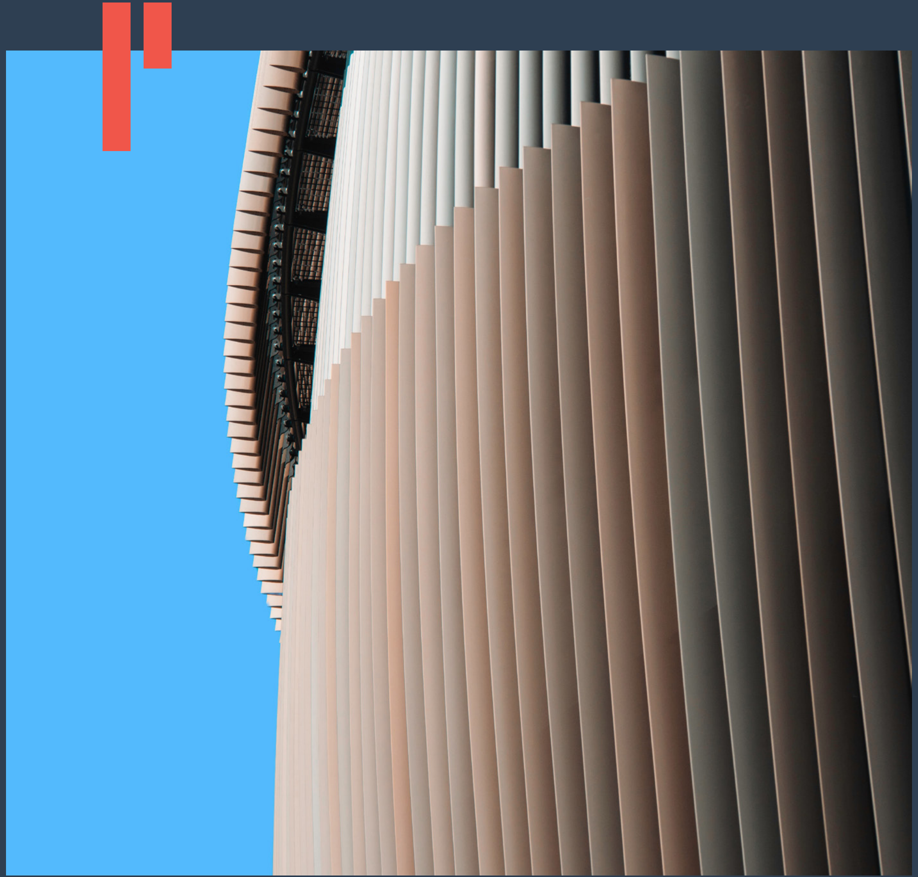
All in-person participants must present proof of a negative COVID test taken the morning of the event. (Photographs are fine. Commonly available rapid self-tests are fine). We encourage you to bring rapid tests from home to take in your hotel room before walking to the venue. However, we will also be providing rapid COVID tests free for all who need them. If you choose to take a rapid test on site, please arrive at 8:15 am EST to allow for plenty of time to test before the first workshop. All registrants will be given a COVID rapid test to use Friday morning before coming to the conference.

All in-person participants must wear a protective facemask while not actively eating and drinking. Please bring with you tight-fitting, high-quality masks—N95, KN95, KF94, and FFP2.

We encourage participants to spread out during breaks and meals, including taking advantage of outdoor seating. The classrooms in the building hosting PLSC this year, Northeastern's Interdisciplinary Science and Engineering Complex (ISEC), are equipped with high quality air filtration systems and the atrium where participants will have breakfast and lunch is cavernous (six stories tall).

Please stay home if you are experiencing symptoms consistent with COVID! We are happy to have you join us remotely.

We will continue to monitor Boston's COVID figures, which are currently on the rise (as elsewhere) and adjust our protocols if necessary.



CONTACT INFORMATION

In the case of an emergency, dial 9-1-1.

Should you require any technical assistance or are having trouble with any of the audiovisual facilities in a workshop room, first speak to the volunteer in the room. If you're having trouble beyond that, please call Conference Manager Nasser Eledroos at 508-948-8113, or email n.eledroos@northeastern.edu

CONFERENCE PROGRAM

DAY ONE

June 2nd, 2022

Session One - 9:30 to 10:45am

VIRTUAL
Using Information Privacy Standards to Build Governance Markets by Pam Dixon & Jane Winn.
Discussion by Julie Cohen.

The voluntary consensus standards provisions of the UPDPA represent an important innovation in information privacy law, but the idea of using voluntary consensus standards to support legislation in other fields is a very well established idea in U.S. and EU law. Because “standards build markets” these provisions could help to lower the cost of compliance for data users while increasing benefits for data subjects by creating compliance safe harbors through transparent, open and accountable processes.

VIRTUAL
Digital Surveillance of BLM Protesters by Lelia Hampton. Discussion by Arpitha Desai.

The paper surveys to moral, legal, and economic issues surrounding state surveillance of BLM protests.

ROOM 138
How Information Privacy is Propertized by Stav Zeitouni. Discussion by Paul Ohm.

In both the past and the present, much is made of the question of whether information privacy should be propertized. This piece argues that the way information privacy has been legislated, propertization is, in several important ways, a descriptive fact already present.

ROOM 432
How Confidentiality Concerns Shape Cybersecurity Investigations by Daniel Schwarcz, Josephine Wolff, & Daniel Woods. Discussion by Jayshree Sarathy.

We interview lawyers, forensic investigators, insurers, and regulators involved in cybersecurity investigations and find that efforts to protect these investigations under attorney-client privilege and work product doctrine have significantly hindered the ability of firms to conduct efficient, candid incident response efforts, as well as the ability of insurers and other third parties to collect robust data about online threats and effective countermeasures. We propose some possible policy solutions for addressing these issues.

ROOM 136
Appropriation of Data-Driven Digital Persona by Zahra Takhshid. Discussion by Felix Wu.

This article argues for the expansion of the tort of appropriation of likeness to include our personal data as part of the modern day understanding of persona and digital identity. It is not arguing for a new tort. Instead, this article relies on the evolution of this common law privacy tort to illustrate why the appropriation tort is still relevant today and can be helpful for data privacy litigations.

ROOM 140
The Cost of A.I. Fairness in Criminal Justice: Not a Big Deal by Ignacio Cofone & Warut Khern-Am-Nai. Discussion by Orin Kerr.

People claim that applying ML fairness constraints reduces meaningful types of accuracy. They're wrong. We run numbers on the COMPAS database.

ROOM 532
Imperfect and Uneven Bargaining: Privacy's Contact Problem by Sebastian Benthall & Aniket Kesari. Discussion by Jody Blanke.

How well does law & economics theory explain the modern digital economy and what gaps remain? We present an internal critique showing how even in environments with low or no transaction costs, economic inefficiencies are still possible because of network effects, and suggest theoretical and policy solutions.

ROOM 632
Privacy's Commodification and the Limits of Antitrust by-Jeffrey Vagle. Discussion by Siona Listokin.

There is a growing body of scholarship exploring how competition law and policy could be used to regulate the treatment of digital data and protect information privacy. This Article argues that that the use of antitrust as a tool for privacy regulation is flawed by its inherent assumption--and acceptance--of privacy's commodification.

ROOM 142
Against Engagement by Neil Richards & Woodrow Hartzog. Discussion by Kate Weisburd.

In this paper, we explore how the concept of engagement might be treated not just as an online metric or as the ideology behind surveillance advertising funded models, but as a concept to be regulated. Developing anti-engagement principles might offer a fruitful way of tackling many of the often bewildering array of human problems attributable to digital platforms.

ROOM 655
Speaking Back to Sexual-Privacy Invasions by Brenda Dvoskin. Discussion by Audra Jamai White.

This paper discusses how tech companies claim to protect sexual privacy as an excuse to carry out their war on sex and how we might fight back. The paper aims at developing a queer/critical theory of sexual privacy.

Break - 10:45 to 11:15am

Session Two - 11:15 to 12:30pm

VIRTUAL
Covering Prying Eyes with an Invisible Hand: Antitrust Law, the New Brandeis Movement, and Privacy by Matthew Sipe. Discussion by Gianclaudio Malgieri.

The increasingly prominent New Brandeis movement in antitrust law hopes, among other policy goals, to use authority over competition to improve consumer privacy. This Article takes a skeptical view of those efforts; somewhat counterintuitively, the more aggressive and structuralist New Brandeis school of thought risks undermining consumer privacy, rather than enhancing it.

VIRTUAL
Online Public Health Misinformation, and How to Tame It by Ira Rubinstein & Tomer Kenneth. Discussion by Daniel Schwarcz.

The Article analyzes underexplored measures for confronting the problem of online public health misinformation, focusing on soft-regulation and regulation of algorithmic amplification. Positioning public health misinformation as an illuminating case study for regulating online misinformation more generally, we argue that these measures can overcome any existing legal hurdles and are better than present solutions.

ROOM 138
The Limitations of Privacy Rights by Daniel Solove. Discussion by Yan Fang.

Privacy laws often rely too heavily on individual rights, which are at most capable of being a supporting actor, a small component of a much larger architecture. This article discusses the common privacy rights, why each falls short, and the types of broader structural measures that can protect privacy in a more systematic, rigorous, and less haphazard way.

ROOM 136
The Civic Transformation of Data Privacy Implementation in Europe by Inbar Mizarhi Borohovich, Abraham Newman, & Ido Sivan-Sevilla. Discussion by Peter Winn.

Recent data protection laws in the EU institutionalize NGO engagement with regulators and enable bottom-up policy implementation. We study tactics and targets of the enforcement actions of twelve European NGOs and map their contribution to policy implementation based on a novel typology for understanding enforcement actions across scope (local vs. transnational) and goals (direct vs. strategic).

ROOM 655
Privacy Qui Tam by Peter Ormerod. Discussion by Roger Ford.

Privacy law is typically enforced by government agencies or through private rights of action, and these conventional enforcement schemes have significant shortcomings. Qui tam enforcement offers a superior alternative.

ROOM 432
Paid Political Messaging in Immersive Reality Environments by Scott Bloomberg. Discussion by Jasmine McNealy.

This paper theorizes about how paid political messaging will be targeted to users in immersive reality environments (such as the "Metaverse") and explains how that practice will significantly exacerbate existing problems caused by microtargeting online political ads. The paper then argues that the First Amendment Speech Clause should not pose a barrier to U.S. governments restricting such targeting.

ROOM 532
Explanations and Meaningful Information: At the Interface Between Technical Capabilities and Legal Frameworks by Suzanne Vergnolle & Dylan Bourgeois. Discussion by Rob Lalka.

This paper attempts to bridge the knowledge gap on Explainable AI (XAI) and meaningful information between the technical and legal communities. It also suggests ways to collaborate on achieving practical solutions that meet regulatory expectations.

ROOM 140
An Evidence-Based Lens on Privacy Values: Evolving Fourth Amendment Standards and Biometric Technologies by Christopher Yoo & Arnav Jagasia. Discussion by Albert Fox Cahn.
This Article proposes a novel framework for understanding the Fourth Amendment that uses an evidence-based lens to illuminate privacy values. This framework is then applied to three emerging biometric technologies (facial recognition, iris recognition, and DNA profiling) to show how the Fourth Amendment challenges that they raise implicate distinct values.

ROOM 142
The Character of Consent by Meg Jones. Discussion by Alexis Shore.

Draft material from a forthcoming book that tells a new history of digital consent through the lens of one of our toughest and longest tech policy debates: cookies. Using STS-inspired legal construction, the book traces the origins of who consents, arguing that the consent dilemma has never been about privacy self-management but instead a problem of international politics.

ROOM 632
Reversing the Risks: Proposing Privacy Protections for Communications Metadata and Telemetry Information by Susan Landau & Patricia Vargas-Leon. Discussion by Sunoo Park.

This paper explores how the collection of metadata and telemetry information is eviscerating the content/non-content distinction, revealing people's personal information, and leaving users without the possibility of having meaningful privacy choices, and providing informed consent. In this context, this paper also attempts to show how the FTC can act to provide users with meaningful privacy choices.

Lunch - 12:30 to 2:00pm

Session Three - 2:00 to 3:15pm

VIRTUAL
Using Special Category Data to Prevent Discrimination: Does the GDPR Need a New Exception? by Marvin van Bekkum & Frederik Zuiderveen Borgesius. Discussion by Aaron Massey.

Does the GDPR need a new exception allowing organisations to collect sensitive data to test their AI system for discrimination?

ROOM 432
The Case for Establishing a Collective Perspective for to Address the Harms of Platform Personalization by Ayelet Gordon-Tapiero, Alexandra Wood & Katrina Ligett. Discussion by Rebecca Wexler.

In this paper we argue that any attempt to overcome the harms created by platform personalization (including misinformation, manipulation, social polarization, subversion of autonomy, and discrimination), must be based on an understanding of the collective nature of data. In order to overcome these harms, we advocate for the creation of meaningful transparency: a collective perspective providing a third party with ongoing insight into the information gathered and observed about individuals and how it correlates with any personalized content they receive, across a large, representative population.

ROOM 136
Privacy for Sale by Christopher Bradley. Discussion by Katherine Strandburg.

This paper is about the conditions under which consumers' private information can be sold by companies. It presents a new body law on that question, derived from reports written by experts that have to be appointed by courts when companies request to sell consumers' private information in bankruptcy; we hand-collected 140 such reports, and we summarize them here.

ROOM 655
Can the Right of Publicity Rein in Facial Recognition? by Jason Schultz. Discussion by Jessica Silbey.

We are currently in the midst of a massive struggle to regulate biometric identification systems, including facial recognition. There are many proposals under consideration, but could the century-old tort of Right of Publicity become a surprisingly effective solution?

ROOM 138
Privacy Standing by Ignacio Cofone. Discussion by Dennis Hirsch.

The paper proposes a three-step test for standing in privacy cases. The test aims to find an alternative to the circuit split building standing on modern views of privacy and literature on privacy harms.

ROOM 140
The Infrastructural Nature of Statistical Imaginaries: Unpacking the Controversy Over Differential Privacy in the 2020 US Census by danah boyd & Jayshree Sarathy. Discussion by Catherine Crump.

This paper uses the controversy around the US Census Bureau's move to differential privacy in its 2020 Decennial Census to theorize the ways in which statistical imaginaries around privacy and accuracy, and the relational dimensions of these imaginaries, uphold the legitimacy of federal data infrastructures.

ROOM 532
Public Purpose Regulation of Digital Platform Markets: Integrating Antitrust and Utility Regulation by Elettra Bietti. Discussion by James Rule.

I argue that current regulatory and antitrust efforts to rein in the power of tech giants in the United States including speech, privacy and competition efforts must be understood must as part of a new vision of public regulation, efforts aimed at embedding public purpose in digital markets. Recognizing the scope of public regulation as an umbrella concept opens up existing digital regulation debates to experimentation and adaptability to new digital questions bridging beyond siloed antitrust and utility dichotomies.

ROOM 142
The Right to Social Expungement by Itay Ravid. Discussion by Jules Polonetsky.

The paper addresses a largely neglected component of criminal justice reform: the (in)ability of individuals who were wronged by the harsh CJS to reenter society due to online newspapers stories about their criminal past. The paper utilizes the case study of survivors of domestic sex trafficking with past prostitution convictions to illustrate the problem, and offers a solution: to restyle the too-quick-to-be-disregarded right to be forgotten (RTBF) and adopt an "American style" RTBF – "the right to social expungement"

VIRTUAL

Regulatory Spillovers: The Case of GDPR by Florencia Marotta-Wurgler. Discussion by Alessandra Calvi.

We measure empirically the effect of GDPR in United States information practices by comparing the regulation's effect in local practices before and after the enactment of GDPR (as measured by over sixty dimensions in the privacy policies of almost 200 firms), and compare the firms' information practices in their E.U. policies to the U.S policies after GDPR. We present some hypotheses explaining our findings and discuss results to specific categories of terms.

ROOM 632

The Managerialization of Search Law and Procedure for Internet Evidence by Yan Fang. Discussion by Jim Graves.

This article examines how internet technology companies respond to search warrants, subpoenas, and other compulsory legal process. It theorizes companies' responses within broader processes of managerialization in the information economy.

Break - 3:15 to 3:45pm

Session Four - 3:45 to 5:00 pm

VIRTUAL

Life, Liberty, And Data Privacy: The Global Cloud And The Criminally Accused by Rebecca Wexler. Discussion by Michael Froomkin.

U.S. policymakers are creating special procedures for law enforcement to circumvent foreign data privacy laws and access cross-border evidence, but no one is creating similar procedures for criminal defense investigators. This profound structural unfairness in the criminal legal system gets privacy backwards; privacy protections ostensibly meant to constrain government power instead specially empower the government while shackling the criminal defense process that is itself supposed to guard against government tyranny.

ROOM 432

A Principled Decision-Making Approach to Smart Tech Governance in Cities by Brett Frischmann & Madelyn Rose Sanfilippo. Discussion by Ella Corren.

We propose an approach to smart city governance grounded in local, contextual norms and scaffolded by key questions to ask throughout smart city planning, procurement, implementation, and management processes. Although we focus on cities, the approach applies to governance of supposedly smart systems more generally.

ROOM 136

Between Privacy and Utility by Jeremy Seeman & Daniel Susser. Discussion by Evan Selinger.

What happens when the neat formalisms and precise abstractions that underpin differential privacy's mathematical results meet the nuance, normative complexity, and messy institutional dynamics of the real world?

ROOM 138

Platforms, Privacy, and Power: How Sexual Privacy Measures Impact Intimate Expression by Danielle Keats Citron, Jon Penney, & Alexis Shore. Discussion by Brenda Dvoskin.

Sexual privacy violations have a profound impact, chilling victims into silence; denying them sexual agency, intimacy, and equality; and eroding trust critical to intimate expression. This paper makes a theoretical and empirical case for a positive expressive impact of both legal and platform-based sexual privacy measures on intimate expression, providing new insights while also addressing law's neglected expressive role empowering victims of online abuse.

ROOM 660 - Reading Room
The Death of the Legal Subject: How Predictive Algorithms Are (Re)constructing Legal Subjectivity by Katrina Geddes. Discussion by Itay Ravid.

As judges rely on algorithms to inform their decision-making, how is the legal subject differently constructed? How does expressive power shift from the embodied individual (sharing their narrative in their own words) to the data capitalist, identifying what weights to assign to different algorithmic factors? And what does the shifting epistemology of legal subjectivity mean for the legitimacy of legal institutions?

ROOM 655
The Failure of Rectification Rights by Hideyuki Matsumi. Discussion by Jocelyn Aqua.

This Article analyzes how data protection laws that offer a right to rectification handle personal data created by automated systems to forecast people's future. I make a case that the right to rectify cannot be exercised effectively if it is about a probable, or possible, but uncertain future.

ROOM 532
Reining in Tenant Screening: A Legal Roadmap by Tinuola Dada & Natasha Duarte. Discussion by Scott Skinner-Thompson.

This paper analyzes the First Amendment legal challenges that housing advocates and policymakers may need to navigate when trying to rein in tenant screening, and especially eviction records, as barriers to housing. It also provides recommendations on drafting eviction record sealing legislation.

ROOM 632
How Efficiency Fails: Procedural Attention to Automated Decision Feedback by Anne Washington. Discussion by Laura Moy.

Organizational efficiency exacts a penalty of time and effort en masse from individuals outside the mainstream, which I call procedural attention. Less visible than a price mechanism but equally salient to the public interest, I suggest that these administrative burdens provide new avenues for analyzing the cost and benefits of automated systems. -- An excerpt from my upcoming book.

ROOM 140
Administering Social Data: Lessons for Social Media from Medical Data by Christopher Morten, Gabriel Nicholas, & Salome Viljoen. Discussion by Ari Ezra Waldman.

Our Article aims to transpose lessons from the set of legal, technical and institutional mechanisms governing the sharing of medical data (which together we term the "medical data settlement") to the problem of sharing social media data. We believe the robust set of institutions around medical data hold valuable lessons for navigating the Scylla and Charybdis of ensuring independent methods of researcher access while protecting user privacy and preserving (or not running afoul of) trade secrecy.

ROOM 142
Data Privacy, Human Rights, and Algorithmic Opacity by Sylvia Lu. Discussion by Andrew Selbst.

This paper discusses how machine-learning algorithms threaten privacy protection through algorithmic opacity, assesses the effectiveness of the EU's response to privacy issues raised by opaque AI systems, and proposes new algorithmic transparency strategies to promote privacy and human rights protection.

Reception - 6:00 to 7:30 pm
Museum of Fine Arts, Boston

Reception Sponsored by the International Association of Privacy Professionals (IAPP).

DAY TWO

June 3rd, 2022

Session One - 9:30 to 10:45am

VIRTUAL

Big Mistake(s) by Tal Zarsky & Samuel Becher. Discussion by Karen Levy.

This article turns to the well-known yet rarely applied doctrine of mistake in contract law. It examines whether mistake may play a role in recalibrating the inherent imbalance of knowledge, power, and sophistication between giant online platforms and individual users. The article demonstrates that with some tinkering, this doctrine might be applied to allow users to revoke their agreements and apply for meaningful remedies.

ROOM 136

Dataset Accountability by Mehtab Khan & Alex Hanna. Discussion by Luiza Jarovsky.

This paper devises a framework to understand the legal and policy issues arising during the development of large AI datasets.

ROOM 432

Data Protection Impact Assessment in the European Union: A Feminist Reflection by Alessandra Calvi. Discussion by Margot Kaminski.

In this article, I address the following research question: Can the DPIA under the GDPR be considered a feminist tool? Spoiler alert: not really. However, it could still serve feminist goals. For that, my suggestions are to incorporate feminist legal methods and intersectionality into the DPIA process and grant data subjects a "right to DPIA".

ROOM 138

Data Protection Doesn't Work: Oversight Failure in Data Processing Figurations by Jennifer Cobbe & Jatinder Singh. Discussion by Peter Swire.

Drawing on the sociological concept of the 'figuration', insights from governance literature, and critical data protection scholarship, we argue that the logic of EU data protection law reflects trends in regulation and political economic organisation which undermine the law's own oversight processes. The effect, we argue, is that data protection law plays a key role in drawing people into data-driven processes of power, production, discipline, and control which they are often unable to resist.

VIRTUAL

Community, Coordination, and Privacy in Public by Richard Warner & Robert Sloan. Discussion by Jordan Wallace-Wolf.

Informational norms are the foundation on which privacy in public rests, but we not build public policy on that foundation because the foundation is incomplete. The missing element is common knowledge, the recursive belief state of parties knowing, knowing they know, knowing they know they know, and so on potentially ad infinitum. Common knowledge is an essential factor in facilitating coordination, and it unites coordinating parties in privacy-in-public-creating communities bound by trust.

ROOM 140

Doughnut Privacy by Julie Cohen. Discussion by Alicia Solow-Neiderman.

This paper explores the implications of the "doughnut" model of sustainable economic development for efforts to strike the appropriate balance between surveillance and privacy.
I will argue, first, that a similarly doughnut-shaped model can advance conceptualization of the appropriate balance(s) between surveillance and privacy, and second, that taking the doughnut model seriously suggests important questions about the uses, forms, and modalities of legitimate surveillance.

ROOM 532

Beyond War Games: Deduction, Interference, and Access-Based Computing Attacks by Kendra Albert, Ram Shankar, & Sunoo Park. Discussion by Aileen Nielsen.

Since the passage of the Computer Fraud and Abuse Act and many similar computer crime laws, many new and impactful kinds of attacks on computing systems have emerged: today, researchers and practitioners are just as concerned about deanonymization, side-channel attacks, adversarial attacks on machine-learning systems, and other methods that do not rely on unauthorized access to a computing system, or otherwise fall within the CFAA's scope. In this work, we examine attacks that do not involve unauthorized access, contextualizing them as one of three main categories of modern attacks, joined by interference and deduction attacks in a novel taxonomy.

ROOM 655
Define Dark Patterns Through FTC Common Law by Daniel Jellins. Discussion by Andy Sellars.

In order to better define and subsequently regulate dark patterns, a tricky online design or user interface, we should use the FTC's body of consent decrees, statements, and rules to understand what is already a violation of current law or not. From that analysis, we see that for the most part these new manipulative designs can be distinguished as either violation of current law or not.

ROOM 632
The Right to be an Exception in Data-Driven Decision-Making by Sarah Cen & Manish Raghavan. Discussion by Edward McNicholas.

Data-driven assessments estimate a target by pattern matching against historical data, but even algorithms that boasts near-perfect performance on average can produce assessments that perform poorly on specific individuals. These failures can lead to decisions that inflict irreparable harm on individuals through no fault of their own, which motivates the need for a new legal right---that we call the right to be an exception---that evaluates the risk of harm, individualization, and uncertainty of data-driven assessments.

ROOM 142
Privacy Nicks: How the Law Normalizes Surveillance by Woodrow Hartzog, Evan Selinger, & Johanna Gunawan. Discussion by Scott Mulligan.

Privacy law's most significant failure is its neglect of smaller, more frequent, and more mundane privacy encroachments, which we call "privacy nicks." Without a firm backstop to prevent privacy nicks from normalizing surveillance creep, there is nothing to prevent a gradual tolerance of maximum exposure.

Break - 10:45 to 11:15am

Session Two - 11:15 to 12:30pm

VIRTUAL
Data Benefit-Sharing: The International Governance of Cross-Border Data Flows from a Social Justice Perspective by Svetlana Yakovleva. Discussion by Tal Zarsky.

This paper focuses on global data governance with a view to creating a system of benefit sharing, the ultimate aim of which is to reduce global inequality that can be caused by the extraction and mining of [personal] data. The article looks at data use from the perspective of value and then whether and how that value should be distributed between communities and societies from which the data was created to achieve greater social justice for populations on a cross-country rather than intra-country level.

ROOM 532
Bridging Notions of Bias from Tech, Law, & Ethics by Elizabeth Edenberg & Alexandra Wood. Discussion by Aloni Cohen.

While there may be an emerging consensus that sociotechnical algorithms should be designed to be fair, computer scientists, legal scholars, and ethicists are likely not speaking the same language when introducing and evaluating proposals for addressing algorithmic bias. In this paper, we analyze differences between technical, legal, and ethical approaches to understanding bias, discrimination, and fairness in order to lay the groundwork for a broader understanding of the underlying harms and the values that individuals, groups, and society at large seek to protect in designing and enforcing fair algorithms.

ROOM 432
Fourth Amendment Notice in the Cloud by Jesse Lieberfeld. Discussion by Brett Frischmann.

This paper examines the problem of unannounced searches in the cloud and the legal and technological frameworks in which those searches operate. Examining the problem through the frames of communications privacy, constitutional history, and Fourth Amendment doctrine, it concludes that the current practice of unannounced searches under ECPA fails to meet the basic notice requirement at the core of the Fourth Amendment.

ROOM 136
Police Secrecy Exceptionalism by Christina Koningisor. Discussion by Christopher Slobogin.

This Article maps out the extraordinary secrecy protections extended to law enforcement agencies. It then examines the doctrinal and policy-oriented underpinnings of this exceptional treatment, finding that these arguments generally fall into one of three buckets: protection against circumvention of the law, protection of citizen or police officer privacy, and preservation of the effectiveness or efficiency of policing. It concludes that none of these proffered defenses justify the powerful informational protections currently extended to law enforcement agencies.

ROOM 655
Interoperable Obscurity by Thomas Kadri. Discussion by Anne Klinefelter.

Data brokers enable interpersonal abuse by making people easier to trace. This Essay proposes a regulatory regime of "interoperable obscurity" to more effectively and empathetically help people avoid abusive surveillance.

ROOM 138
Holes in the Umbrella: A Critique of Privacy as Taxonomy by Maria Angel & Ryan Calo. Discussion by Rebecca Green.

The taxonomical approach to privacy was initially offered as a pragmatic response to definition fatigue—and justified anew as a means to concretize harms for courts and lawmakers—and has seen much praise and relatively little challenge. This essay argues that a taxonomical approach grounded in social recognition has nevertheless come at significant costs. There are limits to social recognition as the sole criterion for what counts as a privacy problem.

ROOM 632
Architectures of choice, or architectures of control? Dark Patterns and Algorithmic Manipulation by Jennifer King, Caitlin Cary Burke, & Eli MacKinnon. Discussion by Steve Bellovin.

While most research and discussion to date on dark patterns has focused on static user interface design patterns, we argue that there's a distinct, fast-evolving class of manipulative design — which we call algorithmic dark patterns — that merits further elaboration, as well as explicit incorporation into a broader conceptual framework for dark patterns. To this end, we propose a deductive approach to identifying dark patterns that's based on a set of shared characteristics common to both static dark patterns and dynamic, algorithmic dark patterns.

ROOM 140
Legacy Switches: A Proposal to Protect Privacy, Security, Competition, and the Environment from the Internet of Things by Paul Ohm & Nathaniel Kim. Discussion by Suzanne Wetzel.

IoT devices give rise to privacy harms in their basic operation; security harms as they age; and environmental harms when they are replaced due to planned obsolescence. We propose, elaborate, and defend a novel, simple, and concrete solution to address all of these problems: every IoT device manufacturer should build a switch into their device called a "legacy switch," that can be flipped by the consumer to disable any smart feature that contributes to these harms.

VIRTUAL
GDPRxiv: Tracking GDPR Enforcement in the Wild by Supreeth Shastri & Chen Sun. Discussion by Bill McGeveran.

Though European Union's General Data Protection Regulation (GDPR) is hailed as a model privacy regulation, details about its enforcement are not well understood. To address this gap, we propose establishing the state of the art (SOTA) in GDPR enforcement, and present the design and implementation of GDPRxiv: an information archival system that collects and curates GDPR rulings, judgements, reports, and official guidances.

ROOM 142
Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law by Andrew Selbst & Solon Barocas. Discussion by Maria Brincker.

We argue that the FTC should use its Section 5 authority to regulate algorithmic discrimination because it can overcome many of the limitations of discrimination law. We also analyze the legality of such a plan, propose that the Commission pursue a common law approach that parallels its data security enforcement actions, and argue that Section 5 enforcement would be at least as preferable as Magnuson-Moss rule making.

Lunch - 12:30 to 2:00pm

Session Three - 2:00 to 3:15pm

VIRTUAL
Variations in Re-identification Risks of Mobility Trace Data in Different Urban Areas and Population Segments by Feiyang Sun & Jan Whittington. Discussion by Susan Landau.

How does privacy risk of location data vary among different urban areas and population segments? This study looks into this question and discusses its implication for the policy and governance of spatial data privacy.

VIRTUAL
The Carpenter Test as a Transformation of Fourth Amendment Law by Matthew Tokson. Discussion by Andrew Ferguson.

This new Fourth Amendment paper contends that 1) a "Carpenter test" has emerged in the lower courts and 2) this test should largely replace the Katz test -- indeed the replacement has already started. More broadly, it examines the uneasy state of current Fourth Amendment law, in which the Katz and Carpenter paradigms overlap and compete in the lower courts, and describes the many ways that courts have attempted to integrate these two frameworks.

ROOM 432
Assessment Integrity: Distance Learning, Consumer Privacy and Student Privacy in Ed-Tech by Madiha Choksi, Yan Shvartzshanider, & Madelyn Rose Sanfilippo. Discussion by Jill Bronfman.

We explore how educational technologies exacerbate tensions between students, educators, and institutions by framing educational consumers as distinct from data subjects and ignoring relevant values underlying assessment integrity in favor of economic extraction and policing of students.

ROOM 136
Usable EU-Compliant Cookie Consent Banners: Is it possible? by Cristiana Santos & Colin Gray. Discussion by Joris van Hoboken.

We evaluate consent banner design through the lens of existing legal frameworks and design evaluation techniques. Through this bi-directional approach, we seek to identify synergies and tensions among design and law that may also have applicability to future regulatory action in the EU and United States.

ROOM 655
Unjust Enrichment: "Standing" Up for Data Privacy Rights by Bernard Chao. Discussion by Jay Stanley.

The equitable doctrine of restitution and unjust enrichment has been recognized by the courts for centuries. Because it focuses on the defendant's wrongful gains instead of the plaintiff's injury, it can avoid the Supreme Court's injury based standing test. Legislatures should take advantage of this feature and expressly include the unjust enrichment remedy in future privacy statutes.

ROOM 138
Privacy's Social Dimensions by Neil Richards. Discussion by Zahra Takhshid.

This paper explores privacy's social dimensions: the ways in which privacy matters as a social value rather than a narrowly individualistic interest. Exploring the ways in which privacy enables relationships, makes social life possible, and nurtures democratic society more broadly, the paper applies these findings to a series of contemporary privacy policy problems in which individualistic understandings of privacy produce unsatisfying outcomes.

ROOM 140
Federalism in the Automated State by Alicia Solow-Niederman & David Freeman Engstrom. Discussion by Ryan Calo.

AI has a federalism problem: Many of the most concerning AI uses are concentrated in state and local governments, where budgetary and political imperatives, dependence on private sector procurement, and low technical capacity make the emergence of meaningful accountability unlikely. We map these institutional and structural challenges across numerous policy areas and grapple with what might be done given the sharp doctrinal and practical limits imposed by American federalism.

ROOM 532
The Right to Privacy in Islamic Context and the Digital Age: The Case of Gulf States by Bashar Malkawi Discussion by Arpitha Desai.

The paper address the concept of privacy in historical perspective from Islamic point of view. Then, the paper tries to build a connection into modern time by analyzing the laws of select Arab countries.

ROOM 632
Integrating Differential Privacy and Contextual Integrity by Rachel Cummings & Sebastian Benthall. Discussion by David Rudolph.

Differential Privacy (DP) is a property of an algorithm that injects statistical noise to obscure information about individuals represented within a database; Contextual Integrity (CI) defines privacy as information flow that is appropriate to social context. In this paper, we explore the integration of CI and DP paradigms to enable contextually situated continuous information design for preserving privacy.

ROOM 142
Humans in the Loop by Margot Kaminski, Rebecca Crootof, & Nicholson Price. Discussion by Claudia Haupt.

How should we think about humans in the loop of algorithmic systems? More deliberately! Slapping a human in it isn't a general-purpose regulatory fix; rather, it creates a range of new challenges.

Break - 3:15 to 3:45pm

Session Four - 3:45 to 5:00pm

VIRTUAL
Taking Emergence Seriously in Law and Technology Regulation by Samson Esayas. Discussion by David Sella-Villa.

Consider the following legal quandaries: a victim of a wrongdoing without a perpetrator, a work of art without an author, or the possibility that the sum of legally compliant behaviors might give rise to non-compliance. Welcome to the world of emergence in law.

ROOM 136
From Transparency to Justification: Toward Ex Ante Accountability for AI by Frank Pasquale & Gianclaudio Malgieri. Discussion by Kendra Albert.

This paper proposes a system of "unlawfulness by default" for AI systems, an ex-ante model where some AI developers have the burden of proof to demonstrate that their technology is not discriminatory, not manipulative, not unfair, not inaccurate, and not illegitimate in its legal bases and purposes. Although the EU's GDPR and proposed AI Act tend toward a sustainable environment for AI systems, they are still too lenient: what we propose is that AI developers, before launching their systems into the market, must perform a preliminary risk assessment of their technology followed by a self-certification "justification".

VIRTUAL
Van Gogh Interrupted: AR/VR Technology, Privacy, and Accessibility Rights by Brittan Heller. Discussion by David Spatt.

ROOM 432
"Public" Wrongdoing and the Limits of the Right to Privacy by Jelena Gligorijevic. Discussion by Olumide Babalola.

When does wrongdoing disentitle an individual to her right to privacy? 'Public' wrongdoing, the essence of which is the betrayal of another or of the community itself, is inconsistent with why we value privacy and the reasons why we protect it: that type of wrongdoing cannot be covered by a right to privacy.

ROOM 138
Governing Mentalities in Technology Policy: Permissionless Innovation vs. The Precautionary Principle by Gilad Rosner & Vian Bakir. Discussion by Pauline Kim.

This paper explores two different philosophies of how to govern emerging technology: 'permissionless innovation' and the precautionary principle. We critique the former, and argue that the latter is essential to prevent long term, difficult-to-detect technology harms to autonomy, freedom of thought, private spaces, and a liberal democratic order.

ROOM 532
When Privacy Becomes Perpetual: How Temporality Influences Users' Initial and Adjusted Self-Disclosure on Social Networking Sites by Zhuoran Jiang. Discussion by Madiha Choksi.

This paper problematizes how users heterogeneously experience time (i.e., temporality) and theorizes the effects of temporality on self-disclosure. The proposed perpetual privacy model integrates both retrospective and prospective privacy management of personal data on social networking sites.

ROOM 632
ε-Differential Privacy, and a Two Step by Nathan Reitinger, Amol Deshpande, & Michelle Mazurek. Discussion by Rachel Cummings.

Differential privacy does exactly what it says it will do, mathematically speaking, but what does that mean to a statute mandating data confidentiality—what is required before legally protected data may be shared? This paper introduces a novel, two-step test which answers that question, providing a translation between the language statutes speak and the language differential privacy speaks, in turn motivating compliance-inspired, private data sharing.

ROOM 655
What is Privacy—to Antitrust Law? by Erika Douglas. Discussion by Kirsten Martin.

ROOM 140
Recording Race in Public Education by Fanna Gamal. Discussion by Anne Washington.

This paper examines the construction of identity through school recordkeeping.

ROOM 142

The Consent Burden: Between Privacy and Consumer Protection by Ella Corren. Discussion by Woodrow Hartzog.

Empty consent continues to be the vehicle that legitimizes digital surveillance and other exploitations in consumer markets and the information economy. This article introduces a new concept for analyzing these markets — The Consent Burden — which is analogous to the regulatory burden, and can be used as a metric for rights/power allocation in markets; accounting for the Consent Burden can change regulatory logic going forward.

info@privacyscholars.org

www.privacyscholars.org

PLSC privacy law scholars conference