The Governance of Smart City Technologies (Internet Law, Meet Local Government Law)

This essay will investigate how local government law (“LGL”), the set of rules that grants and limits the legal capacity of municipalities, affects the way the Internet of Things (IoT) and digital technologies are adopted in cities. IoT refers to systems of sensors, cameras and computers that share data and work together to make decisions. In the city context they are often referred to as “smart city technologies.”

Cities have limited powers. This limits the types of social and economic policies that they can enact. An important argument in LGL scholarship is that their limited power structures also incentivize them to enact particular types policies: Thus, for example, cities that rely on real estate taxes often enact zoning laws that don’t favor public or subsidized housing. Similarly, cities with powers to tax certain forms of consumption incentivize them to attract companies in the service industry to operate in the city as in the bid to attract Amazon’s second headquarters in 2019, which promised to create high-income jobs, even when others were concerned about what the effects that Amazon’s move to a middle-income city could have in local housing markets. This essay will propose that as digital technologies and IoT are increasingly adopted and deployed in cities, both by corporations and the local governments (“LG”) themselves, it is important to understand how LGL empowers, constrains and incentivizes them to shape in certain ways how these technologies are adopted in cities.

LGs are already engaging in the governance of IoT and digitally-powered services: US cities are adopting a variety of rules regarding facial recognition technology - from completely banning it, like Somerville MA, to enthusiastically adopting it with little public oversight, like Plato CA -; they have adopted different regulatory approaches to autonomous vehicles and they set terms in their public procurement contracts about what data can be collected and whether and by whom it can be monetized. Some cities are including data-sharing provisions in local ordinances that regulate platforms operating various services in their cities (like e-scooters or home-sharing) in an attempt to better enforce existing laws on these companies, use this information for city-planning or even open up the data (after anonymization) to try to address some of the concerns that data-monopolies raise about market concentration. These strategies are also shaped by their limited powers: LGs attempts to regulate platforms are challenged in court as companies label themselves internet intermediaries and as some data-sharing ordinances have gotten struck down by judges they have entered private data-sharing agreements with companies, agreements that have little public oversight.

Lastly, digital technologies empower and disempower LGs in new ways: The various ransomware attacks suffered by many US cities in 2019 are an example of this, but they can engage in problematic surveillance practices too.

Many of the challenges and opportunities posed by smart city and digital technologies adopted in cities are well known to Internet scholars: From AI and data governance, to content moderation and how to govern technology companies that can increasingly influence our economies and societies. This essay will present three case studies of LGs engaging in data
governance strategies of the like referred to above as a means to intervene in how IoT is deployed in their cities, and explore what the risks, benefits and potential of these different approaches are. By doing so, it hopes to start mapping sites for regulatory and policy interventions that can lead cities and communities to harness the potentials of their IoT futures, while still protecting them from the abuses of powers that these technologies make possible.

**Beatriz Botero Arcila**  
Berkman Klein Center for Internet and Society at Harvard University / SJD Candidate Fellow / SJD Candidate  
bboteroarcila@sjd.law.harvard.edu
Reasonableness as Censorship: Section 230 Reform, Content Moderation Liability, and Internet Speech Exceptionalism

For the first time in the Internet’s relatively brief history, revising the Communications Decency Act’s Section 230 to permit greater liability for social media platforms’ carriage of third-party content seems to many not just viable, but necessary. Many of these calls are built around the related and longstanding common law liability principles of duty and reasonableness. The use of reasonableness in the Section 230 context would condition the liability of social media platforms on a requirement that the platforms “take reasonable steps to prevent or address unlawful uses of their services.” Duty as a theoretical hook for possible intermediary liability for action and inaction with respect to moderating third-party content is taking hold in the United Kingdom as well, with the UK’s Department for Digital Culture, Media & Sport’s White Paper on Online Harms proposing a regulatory framework for intermediary liability that relies heavily on a “duty of care,” the content of which would be established and overseen by an independent regulator that would determine whether online platforms have acted reasonably with respect to third-party content. These reforms are finding common cause with legislative efforts seeking to compel platforms to adhere to “politically neutral” moderation policies, or else face increased liability. And calls for entirely new regulatory regimes for social media in the United States, with new federal agencies to implement them, advocate for similar approaches.

Using the guidance of the common law to unpack the connections between reasonableness, imminence, and intermediary liability, this Paper argues that these efforts are misguided as a matter of technology and information policy, and so legally dubious that they have little chance of surviving the legal challenges that would inevitably follow their adoption. It demonstrates the many problems associated with adopting a common law-derived standard of civil liability like “reasonableness” as a regulatory baseline for prospective platform fault. It also discusses the challenges that the use of Artificial Intelligence-driven content moderation presents to the task of defining reasonableness, and considers the fit between content moderation and products liability, another common law fault theory increasingly used to argue expanding intermediary liability’s scope. “Reasonableness”-based Section 230 reforms would also lead to unintended, speech-averse results. And even if Section 230 were to be legislatively revised, serious constitutional problems would remain with respect to holding social media platforms liable, either civilly or criminally, for third-party user content.

Enrique Armijo
Elon University School of Law
Associate Dean and Professor
earmijo@elon.edu
The Law of Influencer Marketing

This paper discusses some of the issues that have risen with the use of social media platforms to create influencer accounts. It addresses how strong social media platforms are in controlling the content networks on their sites, and the need for legislation to regulate the responsibilities for social media platforms related to intellectual property.

Husain Bazzi
Brooklyn Law School
Student
husain.bazzi@brooklaw.edu
Hardened Soft Law: The Third Party Effect of the FTC's YouTube Settlement

On September 4, 2019, the Federal Trade Commission announced sweeping regulatory changes to the operation of one of the internet’s most popular websites. This website has 2 billion monthly active users and features content from more than 50 million individual creators, most of whom are small businesses or individuals. Many of the creators affected earn money using the website, and stand to lose, in aggregate, millions of dollars from these regulatory changes; some will need to restructure their business model. The changes also subject content creators to increased risk of stiff fines. Yet these significant regulatory changes were never put before a legislature; none of the content creators or users of the website were privy to the rationale or design of the regulation; and there was no public process for comment. Instead, the new regulation was confidentially negotiated between the website company and agency staff and put into place by a court.

The FTC’s settlement with YouTube over Children’s Online Privacy Protection Act violations has staked out a new and consequential region on the continuum between hard law and soft law. FTC settlements have long been praised by those who value the soft law benefits of such an approach: flexibility to deal with case-by-case specific problems, particularly in fast-changing industries; limited need to set industry-wide rules in place; the ability to shape future behavior through a kind of common law. Such settlements have also long been criticized by those who emphasize the difference between them and hard law: a creation of regulatory ambiguity; lack of process that considers the interests of the full range of stakeholders; a “rulemaking” environment with a power differential between the negotiating parties; and an agency ability to accumulate incremental changes to the law that in total can be quite significant.

The YouTube settlement may be the hardest soft law ever generated through the FTC’s settlement process. It differs from previous settlements in at least four ways. First, the scale of the effect. This has two components: the large number of third-party individuals affected and the significant size of that effect. Previous settlements (such as Equifax or Facebook) have been with platforms with large numbers of consumers involved, but the direct effect on those consumers was much smaller. The YouTube settlement directly compels action by, and raises regulatory risk for, millions of individuals not party to the settlement. Second, and related to the first, it is clear from the complaint that the FTC intended the settlement to address non-compliant behavior by non-settling parties, namely content creators. Typically, the FTC would bring legal actions against non-compliant parties where they would be able to argue their case, but the YouTube settlement will eliminate a large number of non-compliant content creators while making those that remain easier to sue. Third, the YouTube settlement differs from other settlements because it signals significant changes to the FTC’s interpretation of a statute, in this case COPPA. The FTC has authority to change the regulations implementing COPPA and has previously done so, but in APA-compliant rulemakings rather than settlements. Fourth, the YouTube settlement differs from some other significant settlements in that the commission used a process that did not provide any opportunity for public comment on the settlement; many other settlements have had a public comment period. (The FTC had sought comments on the COPPA Rule in July 2019 and extended the comment period after announcing the YouTube
settlement; that comment period is now closed and the matter is pending at the agency.)

This hardened soft law raises many questions. Due process and administrative law concerns about the FTC’s settlement process have been somewhat overblown in the past, but are harder to ignore in this case. Does this represent a new template for FTC enforcement against platforms? How should the FTC adjust the COPPA rule in light of the settlement and the massive feedback from content creators? And the implications of this settlement stretch beyond FTC. In particular, it offers lessons about the effects of imposing liability on a platform for hosting non-compliant third-party content: a lesson that will be increasingly relevant as the battle over Section 230 rages.

FTC settlements have always been hard law for the settling company and soft law for everyone else. The YouTube settlement uniquely expands the hard law effect of an FTC settlement, and the implications are worth exploring.

**Neil Chilson**
Charles Koch Institute
Senior Research Fellow, Tech and Innovation
neil.chilson@charleskochinstitute.org
Make No Law: How the DMCA Offends the First Amendment

Copyright law and the First Amendment do a complicated dance. The former is born of the Progress Clause of Article I of the Constitution granting Congress the power to make such laws, and the latter is a Constitutional limitation then constraining any laws Congress might make. Copyright law therefore cannot exist independently of or indifferently to the restrictions the First Amendment places on any Congressional act, including its passage of copyright law.

At least in theory. In practice, however, while some parts of modern copyright law may be perfectly constitutional, other parts are not. These infirmities, far from being merely theoretical, frequently impinge on the public's First Amendment rights and lead to the wrongful suppression of lawful speech. Thus it's wrong to keep giving copyright law a pass. To ensure First Amendment rights are as effectively protected as the Constitution demands, we need to identify where copyright law has been interfering with those rights, and correct it so it no longer does.

Which is where this paper comes in, to look at some of the ways current copyright law conflicts with First Amendment doctrine, particularly with respect to the Digital Millennium Copyright Act, a 1998 Amendment to the 1978 statutory overhaul of US copyright law and frequent culprit behind much of modern copyright law's resulting harm to free speech.

In some instances the problems are born from the practical application of Section 512 of the DMCA. For example, the pressure a service provider faces to remove content, regardless of whether it is truly infringing, leads to a strong censoring effect, and one that bears the hallmarks of prior restraint: censorship of expression without it having been adjudicated to actually be actionable. And in other instances it is the courts, interpreting the DMCA's provisions, that have given them their unconstitutional quality. The fact that mere accusation of infringement can exacerbate the pressure to censor content, and, worse, cause users to be silenced entirely, is both a creature of careless statutory drafting and widespread judicial indifference to the implications of it continuing to interpret the DMCA's provisions without reference to the prior restraint these interpretations invite. In particular, Section 512(f), which was supposed to deter wrongful takedown notices, has largely been defanged. Worse, recent developments in 512(i) case law have also led to service providers, including full-service broadband ISPs for which there may be no other competing service, to cut users off from the Internet, sometimes entirely, and, again, often on the basis of mere accusation alone and not an actual judicial finding of wrongfulness.

In identifying these sorts of problems the paper also contemplates whether the DMCA can be saved - or, in other words, can it be made to be constitutional - and whether it even should be. And the answer to both questions appears to be yes. It should be yes, because Section 512 is actually a system to protect service providers, who need this safe harbor protection in order not to be even more unduly pressured to censor the lawful expression they intermediate. While it could be good for Congress to take another stab at creating a safe harbor system that is more usable and therefore protective, slight drafting improvements to clarify small ambiguities may do much to cure the severe Constitutional infirmities that have grown from them. For most of the problems with the DMCA are the fault of the courts, which need to be vastly less willing to
interpret the DMCA’s provisions in ways that conflict with the First Amendment in order to ensure that the DMCA does not continue to.

Cathy Gellis
Attorney
cathy@cgcounsel.com
The (European) Artificial Intelligence (R)Evolution: Are Trustworthiness, Law, Ethics, and Robustness, Enough for (Re)Liability?

The European Commission qualifies AI as a “game changer” and a European Independent High-Level Expert Group on AI (AI HLEG) witnesses an “AI driven world.” Every “traditional lawyer and law professor” would expect that if the game and the world changes and a new “driver” appears on the scene (deus et dea et machina?) new law would evolve. Hence, especially (primary) law (on the European Union level) would change as well. However, as we all know, constitutional amendments or an adaption of European Union (primary) law for an AI augmented world (own terminology) or a “robot world” have not materialized yet.

We do not see a mutation, innovation, evolution or revolution of legal systems at present. However, it is necessary to create new legal settings in order to alleviate concerns of the public and of relevant industries alike when it comes to questions of liability for (un-)foreseen negative consequences caused by robots as well as AI systems. Defining robot and AI systems and designing a legal framework for liability are a prerequisite for reliability. A lack of legal certainty threatens to stymie users as well as innovators in the design, production, distribution, merchandising and maintenance sector. Concerns regarding (un-)foreseeable risks (liabilities) and attempts at limiting liability are obvious as well as understandable.

Hence, new and holistic approaches to qualify and evaluate AI systems and robots are of highest importance. The AI world concept of the AI HLEG tackles this innovation barrier in 2019 by establishing the here so called “LER and FRA Formulas.” “FRA” is an acronym for “Foundations,” “Realization,” and “Assessment.” The lawful, ethical and “robust” quality of AI systems (“LER Formula”) gets the meaning of a “Foundation” for a future brand called “Trustworthy AI for Europe.” Not only does this lay the AI Foundation, moreover, it also establishes that technical and non-technical measures have to be used to fulfill these fundamental requirements. Last but not least, the design of a “check-list” for AI is groundbreaking not only for AI systems but also for robots (e.g. autonomous vehicles). This “Assessment List” is currently in the process of interactive governance and feedback. Even in its first version, it might plaster the path towards a new “liability, accountability, responsibility law” for AI as well as for robots (,ÄüEGEGfTAI-I-2019,Äü, p. 26 continuing). Summing up: Creating “ethical” (not legal) rules at the forefront of developments and attempts at escaping traditional legal liability does not suffice if revolution and technophobia are the consequence in the aftermath of (possibly high) risk applications in industry and society. Consequently, the first priority of law (as part of LER) is the development of a liability regime, especially in procedural law (such as administrative and civil procedure). The European Union and the Member States have to face the challenge dealing with “rogue” systems (AI systems that have no connection with a liable subject or that operate outside of causality principles linking a liable human subject [developer, producer, owner etc.] to a harmful outcome due to autonomous choices / behavior). It is a matter of interpretation whether AI is revolutionary or evolutionary, which is why we chose the denomination “(R)Evolution.”

The authors have competencies in German and European Union law and Georg Gesk has excelled in Chinese law as well. For the audience of the Internet Law Works-in-Progress

**Georg Gesk**  
University of Osnabrueck (Germany)  
Professor  
ggesk@uni-osnabrueck.de

**Viola Schmid**  
Technical University Darmstadt (Germany)  
Law Professor  
schmid@cylaw.tu-darmstadt.de
When Algorithms Meet Fairness: Big Data, Price Calculation and the Discrimination Quandary

The algorithmic price calculation becomes an increasingly widespread and meaningful way of organizing business activity on the online market. Some firms (such as Amazon and Uber) provide each customer with a customized price on a take-it-or-leave-it basis. The others (like Airbnb) offer dynamic, tailor-made pricing schemes, based on algorithmic calculation, as an option, hence nudging contractors to adopt particular price floors.

Although the idea of pricing various customers differently is not new as such, it has become substantially transformed and extensively invigorated with the rise of the algorithmic-based tools. The development of massive data harvesting techniques, combined with robust computation skills employed to processing them, does not merely make the price calculation much more sophisticated and multicomponent than ever before. It also opens an entirely new chapter in understanding the relation between the individual on the market and the value of a good or service. In the world of algorithms-enhanced commerce, clients are offered prices on a case-by-case basis, depending on how a machine allocates them against the background of the dataset about the particular population. In doing so, it makes a particular behavioral prediction about and individual, estimating her willingness to pay particular price in the given circumstances (as is e.g. the case of surging prices for car sharing when the weather conditions deteriorate).

Framed in this way, the algorithmic calculation of prices subverts the classic ideas of market justice and transactional fairness: an individual price no longer builds on its objective market valuation, but rather on the way how the machine correlates idiosyncratic characteristics of an individual with the entire dataset. In the further consequence, individuals may receive price that builds on biases embedded in the collection of data or in the design of the algorithm as such. Moreover, the algorithmic price-setting may (straightforwardly or indirectly) reflect individual features that, for fundamental ethical reasons, should not constitute a valid premise for market valuations (such as gender or religion). For these reasons, algorithmic calculation of prices raises serious risk of discriminatory segregation of individuals that may directly lead to their partial or entire market exclusion.

Building on these observations, the paper attempts to delve more deeply into the concept of fairness in the machine-based price calculation and to map its normative ramifications. In particular, it seeks to juxtapose the specific nature of the algorithmic-based price calculation and the classic notions of transactional fairness (with the particular regard to the “fair price” concept). In this respect, it attempts, in particular to understand the dynamics between the “substantive” and “procedural” understating of price fairness and to identify how they interact in the context of algorithms. In this regard, the paper attempts, in particular, to test the concept of “augmented price fairness” which encompasses both the classic ethical premises, as well as the “fair” collection and use of data that constitutes a basis for making behavioral predictions. This attitude, as the paper argues, seems to provide a better-fitting response to the inherent link between operation of algorithms and creation of a dataset.
Upon these premises, the paper tries to critically evaluate the proposals for regulating algorithmic price-setting through increasing procedural guarantees (i.e. mandated disclosure and algorithmic explainability), advocated by scholars and policymakers in the US and in Europe. It seeks to compare and contrast them with more substance-oriented attitudes and to understand the underlying premises for effectiveness of each of these approaches. In conclusion (which is still tentative at this point), the paper argues against purely formal attitudes and draws more case-specific policy proposals for regulating price-calculating algorithms.

Mateusz Grochowski  
European University Institute (Florence) / Polish Academy of Sciences (Warsaw), Information Society Project (Yale Law School)  
Max Weber Fellow (European University Institute), Assistant Professor (Polish Academy of Sciences)  
mateusz.grochowski@aya.yale.edu
Platforms as Blackacres

If in William Blackstone’s time we might have thought of a person’s home as their castle, in Mark Zuckerberg’s time we might say that their website is too. Under cyber-trespass laws like the Computer Fraud and Abuse Act, courts are treating all websites as private “blackacres,” as enclaves of private property that online platforms may govern much like owners of private land use trespass law to exclude people from their property in the real world. The law empowers platforms to act as digital gatekeepers that may grant and restrict access to their websites for any reason whatsoever. This gatekeeper power affects all sorts of actors “from academics to journalists to competitors,” who wish to access websites and gather information that might jeopardize dominant platforms’ reputations or business interests, particularly when researchers want to investigate harms like online discrimination, election interference, or anticompetitive behavior. Faced with this external oversight and competition, platforms are using cyber-trespass law to threaten researchers with criminal and tort liability for gathering information against their wishes.

This legal landscape has also encouraged platforms to develop radically different approaches to managing their relationships with outsiders. Despite the platforms’ policies against scraping, they have selectively waived certain restrictions when it suits them. Facebook cherry-picks particular outsiders by entering into data-sharing partnerships that permit a handful of lucky researchers and businesses to access information on its website. Twitter, meanwhile, sells access to those willing to pay, offering troves of information to those able to cough up. And LinkedIn erects technological barriers to prevent competing services that rely on publicly accessible information about LinkedIn’s users. Despite these differences, however, the principle behind the platforms’ approaches is the same: My house, my rules. The law gives platforms a gatekeeper right to grant or deny permission as they see fit, just as landowners may generally exclude people from their property for any reason whatsoever. Put simply, websites are blackacres.

This Article argues that it is unconstitutional to treat all websites as blackacres under cyber-trespass law. To reconcile cyber-trespass law with the First Amendment, courts should recognize two different types of cyberspaces: cyber-trespass law should have no force on websites that are accessible to the general public, but it should offer robust protections when websites are concealed behind technological barriers that make them inaccessible to the general public. Recognizing a distinction between these types of cyberspaces will protect privacy and speech interests while enabling digital research and oversight. Even if the First Amendment didn’t require this distinction, courts and legislatures should interpret and amend cyber-trespass laws along these lines because doing so is preferable on policy grounds. Applying cyber-trespass rules across the entire internet has insulated platforms from scrutiny and rivalry. To remedy this concerning trend, this Article provides a framework for courts, legislators, prosecutors, and even platforms to avoid unconstitutional and undesirable uses of cyber-trespass law. Adopting the framework would not only satisfy the First Amendment, but it would also help to reinvigorate competition and protect privacy interests that are increasingly threatened in the digital age.
Thomas Kadri
Yale Law School
Resident Fellow
thomas.kadri@yale.edu
Impact of Fake News Through Social Media: Contemporary Issues and Challenges in India

The concept of “fake news” has garnered substantial attention in recent years, evolving from its satirical literary origins into a passionately criticized Internet phenomenon. Whether described as rumours, counter-knowledge, misinformation, post-truths, alternative facts, or just plain damned lies, these false statements of fact typically are published on Web sites and disseminated via social media for profit or social influence. The instances of fake news have become so much that for the first time in India, the National Crime Records Bureau (NCRB) of India has provided statistics on fake news. The statistics provided by the NCRB thus designates “fake news” as a crime. Reports show how there have been instances of 257 reported cases against fake news in India, where Madhya Pradesh has topped the list with 138 cases followed by Uttar Pradesh with 32 cases. The NCRB has included incidences of violence as a result of fake news in their data.

The idea of more effective fact-checking has come up often in the debates around India’s disinformation contagion. But it comes with many conceptual difficulties: A large proportion of messages shared on social networks in India have little to do with verifiable facts and peddle prejudiced opinions. Fake news is not a technological or scientific problem with a quick fix. It should be treated as a new kind of public health crisis in all its social and human complexity. Even if technology giants are subject to severe controls, new methods will emerge to meet the demand. In the short term, a broad antismoking-style campaign against misinformation on social media is likely to be effective. It can win broad political support because ostensibly every political party is against fake news. If we want to preserve the bedrock of liberal society (the principle that ideas of all kinds can be shared in privacy), then the real battleground is not technology platforms or changing the behaviour of politicians but increasing the immunity of citizens.

The Supreme Court Monday refused to entertain a plea seeking a direction to the Centre to frame guidelines and laws to curb the menace of fake news on social sites. A bench headed by Chief Justice of India dismissed the plea which had sought directions to the ministries of Home Affairs, Law, Information and Broadcasting and Electronics and Information Technology to constitute a committee for tackling fake news on various social media handles.

Information Technology Act, 2000 erode digital security and undermine the exercise of human rights globally as it exempts intermediaries from liability in certain instances and states that they will not be liable for any third party information, data or communication link made available by them. “Fake news” is commercially beneficial to the intermediaries and there is a vested interest in the generation and spread of it. There is, therefore, no commitment to eliminate fake news and opposition is mounted only because of this commercial self-interest. Technology here can only be seen as a medium for exchange of mass messages. The end-to-end encrypted platform of WhatsApp here acts merely as a channel for information/misinformation dissemination. It’s important to understand the societal mindset that pushes people to forward such messages. Here lays, the big question of accountability too. This research work presents comprehensive theoretical consideration related to fake news for
purposes of legal analysis and provides a non-exhaustive survey of the many legal and regulatory issues that face fake news publishers.

Zubair Ahmed Khan  
University School of Law & Legal Studies, GGSIPU  
Assistant Professor  
zubairkhan@ipu.ac.in
The Social Elements of Surveillance

In a 2005 Washington Post editorial, Judge Richard Posner famously asserted that there was no invasion of privacy where computers, rather than people, scanned documents and data. His assumption, matching the intuitions of many, is that the social aspect of being watched constitutes the primary harm of surveillance as a privacy invasion. These intuitions are reflected in many areas of law that touch on private spaces, such as limitations on surveillance warrants where access is requested to particularly intimate physical spaces. Social constraints clearly play a role in the acceptability of various forms of surveillance.

However, the full extent of social considerations in legal and lay acceptance of new surveillance technologies has yet to be explored experimentally. This paper addresses that void. In a series of behavioral experiments, we permute fundamental attributes of electronic systems to determine which capacities lay people find objectionable and which less so. We further compare functionally equivalent human and digital computing systems to quantify a preference for digital surveillance over surveillance performed by human agents. Finally, we consider what this strong antipathy to the social element of surveillance predicts with respect to political and legal limits on technologically-powered surveillance. Such questions are particularly important given the ever-increasing surveillance capacities of private consumer-facing firms. We predict that in the absence of new, strong social norms, which are not yet emerging, the ascendance of surveillance-enabling consumer infrastructure will continue.

Outline
I. Socially savvy digital design and its legal implications
   a. The rapidly advancing science of product design
   b. The lagging science of tech regulation
II. Experimentally determined surveillance preferences
   a. Behavioral preferences regarding information storage
   b. Behavioral preferences regarding information transmission
   c. Behavioral preferences regarding humans or digital devices, all else being equal
   d. Some surprising defaults in expectations for different media
III. Prognostications for the digital ecosystem
   a. The product payoffs for reducing socially salient objections to surveillance
   b. The unlikeliness of social responses keeping pace with technological evolution

Sample Bibliography

Aileen Nielsen
ETH Zurich, Center for Law and Economics
Fellow in Law and Tech
aileen.nielsen@gess.ethz.ch
Brazilian General Data Protection Act - An Overview

Brazilian General Data Protection Act (LGPD), Law 13.709/2018, is the legislation that regulates the processing of personal data in Brazilian legal system. Inspired by the General Data Protection Regulation of the European Union (GDPR), the Brazilian General Data Protection Act (LGPD) lays down rules on the collection, processing, storage and sharing of personal data managed by organizations. This law is based on several values, such as respect for privacy, informative self-determination, freedom of expression, information, communication and opinion, the inviolability of intimacy, honor and image, economic and technological development and innovation, free enterprise, free competition, consumer protection and human rights, freedom and dignity. The legislation is inserted in a context of Brazil's progressive adaptation to global data management best practices and covers all companies established in Brazil, as well as foreign-based organizations that offer services or have operations in Brazil involving data processing. Companies that violate this new law will be subject to the application of warnings, fines, blockages, suspensions and partial or total prohibitions on the exercise of their activities. Fines can reach 2% of the organization's revenues, with a limit of R$ 50 million per infraction. The authors of this abstract intend to comment on the main points of this important Brazilian legislation.

Tarsis Barreto Oliveira
Federal University of Tocantins (Brazil)
Associate Professor
tarsisbarreto@mail.uft.edu.br

Cleorbete Santos
Federal University of Tocantins (Brazil)
Professor
cleorbete@gmail.com
Show Me (the Financial Data About) the Money! Big Banks, Startups and the Consumer

In recent years, several U.S. banks have threatened to block technology companies’ servers from accessing their customers’ financial data. These banks have argued that limiting access is the best way to look out for their clients’ best interests and protect their privacy, improve their accounts’ safety, and promote consumer protection principles. The banks have also argued that the technology companies’ apps often collect more data than they need, store it insecurely, sell it to third parties, and do not care enough about people’s privacy, thereby enabling the exposure of individuals’ account numbers and passwords. But the motivation of the big banks in advocating for such limitations may not be so pure. Put simply, banks do not want to be held liable for losses of funds or data, give a competitive advantage to the financial industry’s new entrants, and are afraid of losing customers (and the fees they pay) to innovative technology companies.

Witnessing this push against them, technology companies have not been sitting idly, waiting for the incumbent financial institutions to reduce their access to or to pull the plug on data entirely. They have been actively working on high-tech ways to outsmart and out-maneuver banks’ blocking technology. But they have also extended the fight beyond technological innovation and into Washington. Indeed, technology companies have been strongly lobbying for a top-down approach to open banking in the U.S., which, inter alia, would enable consumers to have the right to give consent to regulated third party providers to securely access their financial data.

The legal status of third parties’ right to access consumers’ financial data is anchored in the EU’s recently adopted Payment Services Directive II (PSD II), and in other parts of the world, but is much murkier in the U.S. While the EU is focused on empowering consumers to decide regarding their financial data, the American approach has been, thus far, a market-based one. However, this status-quo could change. The Dodd-Frank Act’s Section 1033, which “provides for consumer rights to access financial account and account-related data in usable electronic forms” has not yet been judicially interpreted. So, its applicability to consumer-authorized data access, by third parties, as opposed to consumers’ direct access, is still at question. This Article examines the rationale behind the different possible interpretations of Section 1033, and explores this banks versus technology companies’ rivalry from the perspectives of the two pillars of financial regulation, prudential regulation and consumer protection. It also examines the issue of open banking through a comparative lens, discussing the pros and cons of a top-down and a bottom-up regulatory approaches. Finally, it offers suggestions as to what an ideal framework to addressing open banking could be.

Nizan Packin  
City University of New York  
Associate Professor  
nizan20@gmail.com
An Appraisal of the Legal Regime of Internet Policing in Nigeria

The emergence of the internet has created so many opportunities, communities, individuals, governments and businesses are legally availing themselves of the increasing sophistication and utility of the internet. The waves of this innovation has touched all spheres of human life. In spite all this, the cyberspace which is the creator of the internet has come with a number of challenges. It presents a new frontier for criminology by introducing a new form of deviance, crime and social control. Cyberspace is changing the nature and scope of offending and victimization. The police are powerless in addressing the challenges posed by the emergence of the internet, even though there are frantic efforts and measures taken especially by developed countries to arrest this menace through internet policing. In Nigeria, the situation is entirely different. Therefore, the focal point of this paper is to examine internet policing with particular reference to Nigeria. The paper will unravel some of the challenges face via internet policing in Nigeria. The methodology to be adopted is doctrinal. The paper will conclude by making recommendations on how Nigeria will utilise internet policing in tackling crime.

Ibrahim Shehu
Usman Danfodiyo University Sokoto Nigeria
Lecturer
canalilly2@yahoo.com
Digital Trade and Artificial Intelligence: Role of Intellectual Property

In the era of globalization the Artificial Intelligence (AI) emerged as a most accepted technology with its application in various field throughout the economy and society. In coming years growth of AI is impediment and it’s going to have a significant impact on the creativity, production and distribution of goods and services in the market. The present research proposal is aimed to study the intellectual property issues in relation to AI in digital medium. The digital transformation around the globe and data based business method paving the way for its affects in all aspect of our day to day lives. For examples, smart product and services, machine learning, autonomous processes in logistics and production etc. The process of digital transformation is complex and based on multiple layers of technology based on cyber-physical systems (CPS). In CPS physical and software components are closely intertwined and are enabled through the Internet of Things, which allows object to collect and exchange data, resultant is the sensors, actuators controlled the device remotely across the existing network infrastructure. The digital transaction and business methods are considered to be more efficient and accurate which gives more economic benefit.

The companies developing these programmes are trying to make their presence by leading more innovation and automation in technological and digital business. As an incentive to technological innovation and to reap the benefit of investment it is essential to own and protect the Intellectual Property in all innovations. The ownership of intangible aspects of software innovation and data protection is a difficult question and different Intellectual Property mechanism recognized under WTO TRIPS including copyright, patents and design are examined in the research for better and effective protection of software innovation. Protection of data is an important aspect and critical component of AI as its functioning mechanism is based upon machine learning techniques that use data for training and validation. In the present research author is facing difficulties in finding effective protection of data since they are generated by diverse range of devices and activities. In different economy multiple legal frameworks been practiced for protection of data depending on the interest or value. In the context of intellectual property the existing IP system provide protection to data in the form of patent if data represents new, non-obvious and useful innovation. Industrial designs regime protect new or original created data. Under copyright original literally and artistic work represented through data are protected. Data that are having edge over business models in the same area and are not disclosed may be protected through system of undisclosed information. The present research is trying to assess the efficiency of IP laws for protection of digital trade and whether new policy is required under existing IP system for effective protection due to revolution in digital world by increasing use of AI and digital trade. The present study is also focusing on the aspect that any new or existing policy in IP should encourage the free flow of data for uninterrupted functioning of AI without affecting the right to privacy or security.

Dr. Vandana Singh
USLLS, GGSIP University (Delhi, India)
Assistant Professor
vandana.singh@ipu.ac.in
Against a Fairness Doctrine for the Internet

Must social media, search engines, and other online intermediaries be politically neutral under existing law? Or, should existing laws be changed to require such neutrality? Leading American conservatives have made both arguments. Some argue that “Big Tech platforms” may be tantamount to either common carriers or “public for a” to which individual users, publishers or politicians may demand constitutional rights of access, superseding the editorial discretion of the operators of these sites and services. Others argue that such requirements should apply as prerequisites for protection against liability for either hosting or moderating user-generated content under Section 230; either that the law al-ready requires that websites be “neutral public for a” or that Section 230 should be amended to do so. A number of theories have been proposes as to why Section 230’s protections should not apply to social media, including that such websites do not meet the definition of “interactive computer service”; that the term “otherwise objectionable” in Section 230(c)(2)(A) (protecting content removal decisions) should not be interpreted to include removal for political reasons; that such decisions would not constitute “good faith” required by that subsection; and that either aggrieved users or publishers, the Federal Trade Commission or state attorneys general may sue social media sites for failing to deliver the “neutral” service they promised. This paper will explore and deconstruct each of these claims, building upon testimony delivered by the author in testimony on this issue before the House Judiciary Committee in April 2018. It will also explore historical parallels, most notably the Fairness Doctrine applied to broadcasters by the Federal Communications Commission 1949-87, and how various proposals for a “Fairness Doctrine for the Internet” could be abused.

Berin Szoka
TechFreedom
President
bszoka@techfreedom.org
Disambiguating “Cybersecurity”

Cybersecurity is perhaps one of the most poorly-defined and “overloaded” professional terms-of-art in contemporary society. Heavily used by policymakers, business leaders, professionals, and academics, the term “cybersecurity” in popular media evokes images of technical systems, adversaries, criminals, foreign actors, and surveillance issues. Which is precisely the problem: even this simple example of responsive imagery still involves many different possible definitions of cybersecurity. Terms emerging from these meanings include privacy, cybercrime, cyber warfare, data protection, computer security, and numerous other related sub-topics. Some of these terms are used interchangeably, and all are poorly-defined across disciplinary, political, and sectoral silos.

Scholars such as Derek Bambauer and Jeff Kosseff have described various aspects of this problem over the course of the past decade. Bambauer argued that privacy and security are not opposite ends of a spectrum, but rather distinct concepts which may not even inherently be in tension with one another. Kosseff developed a framework for understanding cybersecurity law, based on the classic computer security model of Confidentiality, Integrity and Availability. He argued that while much law exists pertaining to the confidentiality aspect, the integrity and availability aspects are under-addressed in current law. Others have variously touched on these topics in their work over the past decade.

There has been a tremendous explosion in public discourse about the law and technology issues variously titled as “cyber” issues over the past decade. Remarkably, however, legislative, administrative, and judicial fora have largely failed to address fundamental definitional issues of what words like “cybersecurity,” “cyber warfare,” and “data security” mean. Cybersecurity is perhaps the most prevalent example. It appears as a term in discussions of virtually every topic ranging from consumer and individual privacy rights to civilian criminal law to the law of armed conflict, yet rarely appears to have a consistent definition. Put simply, talking about cybersecurity has become a little like talking about God: everyone knows what they each individually mean when using a word describing a higher being, but they don’t necessarily know what anyone else means.

Effective discourse about a topic, however, requires a common language. Discussing how to “improve” cybersecurity will, at best, fail to produce results if some parties are talking about relations among sovereign nation-states and others are talking about the responsibilities of private companies to protect consumer data. (At worst, ineffective legislation that weakens the overall security of our computing and information systems could result.) This Article develops a workable framework for understanding the various areas of law in play in these discussions, how they interrelate, and how to “disambiguate” cybersecurity in the context of the doctrinal framework of U.S. law.

This Article proceeds, in four Parts. Part I examines existing legislative activity, agency action, judicial opinion and scholarship to illustrate the numerous contexts in which variations on the term cybersecurity are used with different meanings. Building from the Bambauer-Kosseff line of scholarship, Part II proceeds to develop a technologically- and legally-consistent proposed definition for the term “cybersecurity.” Part III applies this definition to map the contexts
illuminated in Part I on to existing doctrinal areas of U.S. and relevant international law. Finally, Part IV uses this mapping to illustrate how to understand cybersecurity law (and, indeed, cybersecurity itself) as a complex system with many parts that share a common underlying goal quite familiar to the law: managing risk and expectations.

David Thaw  
University of Pittsburgh  
Associate Research Professor of Law and Assistant Research Professor of Computing & Information  
dbthaw@gmail.com
Privacy as Privilege

On July 26, 2019, a San Francisco judge held Facebook and Twitter in contempt for refusing to disclose evidence subpoenaed by two criminal defendants, despite being ordered to do so by the trial court, the appeals court, and the California Supreme Court. The judge explained, “Facebook and Twitter appear to be misusing their immense resources to manipulate the judicial system in a manner that deprives two indigent young men facing life sentences of their constitutional right to defend themselves at trial.” That was but one of an unknown quantity of criminal and civil subpoenas that have been denied, or chilled from service in the first place, based on the view that the Stored Communications Act (“SCA”) bars private persons from subpoenaing technology companies for the contents of user communications. Litigants may still enforce a subpoena if the user consents, or may subpoena the user directly. But those avenues are sometimes unavailable, such as when the user refuses consent; cannot be located; has a Fifth Amendment, reporter’s, or other privilege against production; or where notifying the user about the investigation could lead to the destruction of or tampering with evidence, to flight, to witness intimidation, or to a threat to life or safety. This Article addresses those cases.

The view that the SCA bars private subpoenas for communications contents rests on “seemingly settled” body of law. The plain text of SCA Section 2702 restricts service providers’ “voluntary disclosure of customer communications.” In 2006 in O’Grady v. Superior Court, a California appeals court construed that confidentiality requirement to immunize service providers from private subpoenas. Every appellate court to have considered the issue since, including the Ninth Circuit, the Second Circuit, and multiple state supreme courts, has adopted O’Grady’s reading of the statutory text to block subpoenas from private persons, including both civil litigants and criminal defendants.

This Article explores a novel theory that the current consensus view of the SCA subpoena bar may be incorrect as a matter of law. Part II presents the argument as follows. When courts construe the confidentiality requirement of Section 2702 to block subpoenas, they create an evidentiary privilege. Creating privilege is a serious matter. Privileges block relevant evidence from the truth-seeking process of adjudication. They do so not because the evidence is unreliable or prejudicial, but rather to serve extrinsic policy goals - such as privacy - that are deemed more important than a full presentation of evidence to the court. Because privileges “are in derogation of the search for truth,” courts must construe them narrowly. Accordingly, detailed interpretive rules control when courts may, and may not, construe confidentiality statutes to create privileges. There is at minimum a colorable argument that the consensus view of the SCA violates these rules. Part III examines the rules’ historical evolution and present instantiation and explains how they might invalidate O’Grady. In Part IV, I consider policy proposals for and against a medium-specific evidentiary privilege for electronic communications, should Congress choose to modify the SCA to enact one expressly. Finally, Part V addresses the implications of these rules for Internet law and scholarship more broadly. Legal scholarship about investigations and data privacy have focused primarily on law enforcement. This Article contributes by examining similar tensions in civil and criminal defense investigations. Ultimately, this Article makes the case that, in some circumstances, privacy law is privilege law, and vice versa. This insight not only carries potentially outcome-determinative doctrinal payoffs, but also opens centuries-long debate over privilege law as a
resource to help inform contemporary debates over tradeoffs between data privacy, security, and transparency in Internet law and beyond.

Part I: The consensus view that the SCA bars private persons’ subpoenas for communications contents in both civil and criminal cases, cases and consequences.

Part II: Why the SCA subpoena bar creates an evidentiary privilege.

Part III: When confidentiality statutes can create privileges, and why the SCA might not qualify.

Part IV: Policy proposals for and against a medium-specific privilege for electronic communications.

Part V: Implications for Internet law and scholarship.

**Rebecca Wexler**
Berkeley Law School
Assistant Professor of Law
rebecca.wexler@berkeley.edu
Algorithm Optimisation and Limits of Human Imagination

This presentation would be an update of the paper that was presented at the Internet Law Works in progress last year and would provide an insight into my recent discoveries concerning civil liability, due standard and stochastic optimisation of advanced algorithms. These ideas will be published for the first time this summer.

In a nutshell, I have based my research on different liability structures for different types of algorithms (deterministic algorithms, supervised learning algorithms and unsupervised learning algorithms). Through this systematization I wanted to visualize why we need different liability rules for different kinds of assignments. At the conference, legal aspect of foreseeability will be discussed along with a description of program’s life circle and programmer’s duty to interpret and debug. The core question is, what duty of care the programmers owe to the customers to provide secure program. The general opinion is that those who develop software and computer systems are in the best position to prevent a potential harm that might appear as a result of the operation of advanced programs. In the case of machine learning programs with continuous self-learning capabilities, it is very difficult to define what is the standard of care imposed on the programmers. With the insertion of new data and introduction of a new environment in which the program needs to operate, a programmer’s standard of care cannot remain constant, it rather depends upon the number of unknowns in the equation, and upon the effects of such unknowns (stochastic problem). It is impossible to expect or require the program to be error-free. From the liability aspect, it is important that it meets the required standard of a reasonable programmer. This standard should vary according to the type of machine-learning programs/algorithms, their classification as good or as service and the possibility of emergent reactions. While making my doctoral research, I came up with the idea that it would be unreasonable to classify a program per se either as a good or as a service. Such classification should depend on its characteristics/type of a machine-learning program and the interventions of a programmer. In practice, it is arguable that a programmer/producer knows or should know, not only the flaws in his/her product, but also the possibility of emergence of errors due to “lifelong/continuous-learning” nature of the advanced machine learning algorithms and potential injuries that are likely to arise.

In theory, programming could be described as the process of translating a particular task into series of sub-sequential commands that helps the computer to solve the task. Creation of the program that can produce a machine-learning solution for a real-world problems requires multiple investigations, corrections, repetitions, predictions of the events (!) and improvements until it reaches the expected and satisfactory performance. The programmers do not know how many repetitions are actually needed in order to prevent the program to produce unsatisfactory outcome/emergent reaction and which debugging tools will improve the investigative process. Important critical value that is enabled by interpretability is the provision of safety. It is believed that only through interpretability machine learning models can be debugged and audited, which is a “precondition” to provide safety. Programmers of machine learning algorithms often use stochastic optimization method with which they provide the algorithm with optimization problem that involves random objective functions or random constrains. In order to prepare an algorithm to the emergence of surprising events algorithm might dealing with in the future (while operating) the programmers face the machine-learning algorithm with
an experimental problem. But how difficult it is to predict all the potential problems or events that may occur during the operation? Is this even possible if we take into account life-long learning capabilities of machine-learning algorithms? Lack of safety standards in the world is the reflection of the nature of advanced programs. It is difficult to say that programmers did something wrong, they might just stop investigating too soon. But what is the standard, where should they stop? How should programmer’s due diligence process be defined? Identifying all potential outcomes the program might produce, deems to be problematic due to limits of human’s imagination.

Therefore, interpreting and setting the sufficiency level of the understanding of a program’s operation deepens and extends the scope of the research to the subjective concept of interpretation/understanding that needs to be objectified with clearly defined duty of care required at different stages during a program’s life cycle, all for the purpose of legal regulation of self-learning programs.

**Tjasa Zapusek**  
University of Zurich, IBM Ireland  
Lawyer/Attorney, PhD candidate  
tjasa.zapusek@gmail.com
A New Proposed Rule for Disparate Impact in Housing

One of legally-recognized discrimination format: **Disparate Impact** was first established in *Griggs v. Duke Powers* (1971). Title VIII of Civil Rights Law of Act of 1968 (Fair Housing Act) prohibits discrimination in the sale, rental or other housing-related activities on the basis of the many known protected classes. But until 2015, the court first included disparate impact doctrine into the Fair Housing Act in *Texas Department of Housing and Community Affairs v. Inclusive Communities Project* as a three-part burden shifting framework:

1. The plaintiff establishes a prima facie case by alleging the discrimination-effect as a fact for its specific practices and providing statistical evidence.

2. The defendant must establish the claim that “the challenged practice is necessary to achieve one or more substantial, legitimate, nondiscriminatory interests.”

3. The burden shifts back to the plaintiff. And the plaintiff must prove that “an available alternative practice that has less disparate impact and serves as legitimate needs.”

The Department of Housing and Urban Development (HUD) is a federal agency which serves as a crucial role to enforce The Fair Housing Act nationwide. But its recent Notice of Proposed Rulemaking (NPRM) claims to write a new burden-shifting framework for establishing disparate impact claims under the Fair Housing Act. This presentation argues that the NPRM distorts the ruling in *Texas Department of Housing and Community Affairs v. Inclusive Communities Project*, and adds to plaintiff’s burden by requiring plaintiff to prove that the challenged practice is “arbitrary, artificial, and unnecessary”. Furthermore, NPRM provides the wrong testing for the algorithm users (for example, tenant screening company) by only asking for the algorithm to be statistically-sound and exclude the protected classes or its proxies from the model’s input. This testing ignores the fact that machine learning models could have disparate impact even without including protected classes and its proxies and will allow for relevant models unexamined.

*Arroyo vs CoreLogic* is a recent and still ongoing case during which tenant screening company (CoreLogic)’s algorithmic product (CrimeSAFE) was sued for violating the Fair Housing Act. As an application of disparate impact testing in housing, *Arroyo vs CoreLogic* serves as a solid part of establishing the disparate impact testing for housing-related algorithm users. By talking about its recent progress, the presentation will explore several important points used for algorithm disparate impact in the housing context.

**Viola Zhong**
New York City Commission on Human Rights; Media Democracy Fund Technology Fellow
xz1809@nyu.edu