Sowell Supporting Documents

This bundle of supporting documents contains the following:

1. cover letter
2. letter of support from Severin Walker, Board Chairman of M^{3}AAWG
3. letter of support from Peter Cassidy, Secretary General of the APWG
4. writing sample, *Operational Epistemic Authorities in the Internet's Infrastructure*, under review by *International Organization*
5. syllabus for *A Nontechnical Introduction to Cyber Policy*
6. flier for advertising the course *Data Science and Visualization for Policy Analysis*
7. syllabus for *Data Science and Visualization for Policy Analysis*

If you have any questions about these supporting documents, please do not hesitate to contact me at jesse.sowell@gmail.com. Thank you for your time and interest in my work.

Jesse H. Sowell II

Department of Science, Technology, Engineering, and Public Policy
University College London

Dear Faculty Search Committee,

I am writing to express my interest in the position of Lecturer in Digital Technologies and Policy with the Department of Science, Technology, Engineering, and Public Policy (STEaPP) at University College London. I am currently an Assistant Professor of International Affairs in the Bush School of Government and Public Service at Texas A&M University. My interdisciplinary PhD in Technology, Management, and Policy from MIT's Engineering Systems Division combines computer science, international political economy, and operations strategy. My research explores the political economy of Internet infrastructure and security. Building on extensive fieldwork, I explain and evaluate how operational epistemic communities managing the Internet's infrastructure create and sustain the knowledge and rules necessary to keep pace with technological change, emerging security threats, and demands for diverse online services. The role these communities play in Internet governance and maintaining a resilient Internet infrastructure has been under-explored in both literature and practice. The insights from my research are essential to systematically and effectively integrating the technical and operational knowledge these communities generate about Internet resilience into evidence-based policy making and the global governance system. Over the past ten years, my engagement with these communities has created regional and global impact, including helping to build cybersecurity communities in developing regions and addressing cybersecurity data governance challenges.

Integrating research, engagement, and teaching is key to understanding contemporary and emerging challenges facing Internet infrastructure governance and security, and for preparing the next generation of sociotechnical policy analysts and researchers to solve global challenges such as cybercrime, platform governance, and improving Internet infrastructure in developing regions. Over the past four years, I have successfully led the Cyber Policy Concentration (CPC) in my department's Masters of International Affairs, single-handedly designing, developing, and delivering this advanced specialization from scratch.

My current and emerging research, ongoing industry and policy engagement, and well-developed cyber policy curriculum are exceptionally well-suited for STEaPP and the Digital Technologies Policy Lab (DTPL). My current work on cybersecurity and Internet infrastructure governance is already a very good fit with ongoing work in the DTPL and the PETRAS National Centre of Excellence. My current projects complement this work, focusing on new dimensions of Internet infrastructure governance not yet explored in the DTPL, such as the politics of submarine cables critical to Internet communications, and the relationships between technology transfers, Internet shutdowns, and autocratic regimes. My ongoing research evaluating Internet infrastructure development in Africa and Latin America complements broader work in STEaPP's infrastructure and development research clusters. I am also developing two new projects on co-regulatory approaches to combating disinformation and data governance that would make a novel contribution to STEaPP's research portfolio. My teaching portfolio is also extremely well-suited for STEaPP, and can be easily adapted for its education programmes. I designed the CPC explicitly for social scientists, from diverse disciplinary backgrounds, interested in developing rigorous technical and policy understandings of digital technology issues.

My intrinsically interdisciplinary portfolio is a rare and valuable complement to STEaPP's mission and programmes, and I believe STEaPP is where I can make the most impact, enhancing my research through collaboration with others, and continuing to innovate in my teaching and external engagement programmes. The next sections describe how I meet the personal specifications for this role in more depth.

Research

My research strategy has always been interdisciplinary. I started my academic life in computer science as a software engineer, focusing on programming language design and network security, but soon realized technical knowledge alone was insufficient to understand the complex sociotechnical dynamics shaping Internet development and cybersecurity challenges. My doctoral research at MIT combined international political economy, operations strategy, and computer science to conduct extensive fieldwork examining on-the-ground practices and policies in Internet infrastructure management and cybersecurity. I funded the last year of my dissertation work as the primary author of a Google Faculty Research Award ($85,000).

As a Postdoctoral Cybersecurity Fellow at Stanford, I won two grants (totaling $125,000) evaluating the informal collaboration between global cybersecurity communities and law enforcement. I developed and executed the research plan; managed budgets and research assistants; and ran workshops and focus groups bringing together cybersecurity professionals, law enforcement, lawyers, and policymakers in the US, Africa, and Europe. This work concluded with a confidential *Combined Capabilities* report evaluating the credibility and legitimacy challenges facing collaborations between cybersecurity "trust groups" and domestic and international law enforcement. The report continues to be requested by partners in private threat intelligence and law enforcement. In collaboration with colleagues at the Shadowserver Foundation, we are continuing this work in a report for Europol. This report documents and evaluates the technical, legal, and coordination challenges during the Avalanche botnet takedown, one of the largest concerted applications of Mutual Legal Assistance Treaties to date.

My research has three common themes, applied to digital technologies policy and governance challenges: *(1)* the coproduction of expert knowledge, *(2)* how it facilitates the kinds of adaptation necessary to keep pace with changes in technology and emerging security threats, and, importantly, *(3)* how to integrate expert knowledge into policy development, regulatory design, and global governance processes. My chapter on planned adaptation in Decision Making Under Deep Uncertainty presents a generalized model for evaluating ad hoc and systemic planned adaptation in the regulation of complex engineering systems. In collaboration with Dr. I. Brass, our article in *Regulation & Governance* presents a planned adaptive regulatory framework for IoT security regulation and standards. My article in the *Journal of Cyber Policy* (featured in a panel at Chatham House in December 2019) comparatively evaluates consolidation in digital platforms, highlighting how governance and accountability strategies employed by communities in the Internet's infrastructure preclude the predatory practices typically associated with platform consolidation. In an article currently under review with *International Organization* (included as a writing sample in this application), my empirical and theory contributions to the Internet governance and epistemic communities literatures provide novel insights into how to integrate critical knowledge produced by the regional Internet registries and the routing community into the global governance system. I believe my core research interests are exceptionally aligned with STEaPP's mission to mobilise deep expertise in complex engineering systems and policy to solve wicked global policy problems.

To coordinate across recently funded research projects, I set up the Internet Infrastructure and Policy Research Group (IIPRG) where I supervise four masters-level student researchers. My IIPRG projects include *(1)* the politics and governance of submarine cables critical to Internet communication; *(2)* mix-methods modeling of the relationship between types of autocracy and Internet shutdowns, with technology transfers as an intervening variable; *(3)* studies of Internet infrastructure development in developing regions, with a special focus on Africa and Latin America; and *(4)* multilevel network analyses (combining organizational and individual ties) evaluating the globally diverse institutional complex that ensures the stability, safety, and security of the Internet, identifying critical gaps between this dense institutional network and the broader global governance system. The submarine cables work has produced one student-authored publication in the Journal of Policy and International Affairs; I am co-authoring a second article on the regional economics and security of submarine cables, under review by

Contemporary Security Policy. The shutdowns work has produced a co-authored, five-case article on autocracies and Internet shutdowns under review by the Journal of Peace Research; to further refine the model, the sequel (in progress) takes a mixed methods approach, using hierarchical clustering to identify trends and threshold cases in global shutdown data from 2016 to 2021. These research streams would not only enhance the DTPL's portfolio with novel and impactful research, but also create fruitful linkages with STEaPP's infrastructure and development research clusters. Interdisciplinary research environments are my native habitat, and I am excited at the prospect of collaborating with colleagues in the DTPL, PETRAS, and across STEaPP on these kinds of projects.

External Engagement and Impact

My novel, empirically rich research findings would not be possible without continuous and trusted engagement with the epistemic communities managing the Internet's infrastructure and security. In the last ten years I have interviewed over 100 actors across these communities, at over 40 network operations and cybersecurity conferences around the world. Since completing my PhD, my engagement is best categorized as impact-driven science and technology diplomacy. By demonstrating I speak technical, policy, and business vernaculars, I have established a reputation as a trusted honest broker that brings a deep understanding of the complex, sociotechnical governance and management problems endemic in establishing collaborative engagement between these transnational institutions, policy makers, regulators, and law enforcement. I have developed rare (and hard won) access to diverse formal and informal institutions critical not only to combating cybercrime, but that also provide the access and empirical evidence necessary to developing deep understandings of the kinds of collaboration necessary for keeping pace with continuous innovation by cybercriminals.

As a Research Fellow and Advisor to the Anti-Phishing Working Group (APWG), I chaired the 2018 Symposium on the Policy Impediments to e-Crime Data Exchange, bringing together cybersecurity experts, lawyers, and policy-makers to highlight the GDPR as an opportunity to resolve the tensions between operational security groups, advocacy groups, and data protection authorities wrestling with tensions between privacy and security challenges. APWG's Secretary General Peter Cassidy recently shared that a number of participants from the 2018 Symposium indicated it was one of the most impactful meetings they have attended. This year we are continuing this work, planning an annual series of Cybersecurity Data and Governance Symposia to kick off in November 2022. Also, in collaboration with the APWG and Dr. L. Weissinger at Tufts' Fletcher School of Global Affairs, we are evaluating the perverse incentives created by ICANN's ill-conceived GDPR compliance. The research findings will contribute to a collaboration with Senator Ed Markey's (D, MA) staff to develop model legislation to ensure the accessibility of data critical to cybersecurity incident response.

Since 2016, as a Senior Advisor to the Messaging, Malware, and Mobile Anti-Abuse Working Group (M^{3}AAWG), I worked with the M^{3}AAWG Board to redesign their Outreach initiatives, creating and leading programs developing anti-abuse capabilities and capacity in Latin America and the Caribbean, Asia Pacific, and Africa, considering each regions' culture, values, and resource endowments, including critical support for engagement with regulators, law enforcement, and international organizations. I am also the co-chair of M^{3}AAWG's IoT Special Interest Group (SIG), working with Internet Service Providers (ISPs) to understand and evaluate the feasibiliy of IoT reputation models. Supporting letters from APWG and M^{3}AAWG leadership are included with this application.

Working with global partners in the cybersecurity, law enforcement, and policy communities, I apply my research on collaboration and governance to support the development of impactful organizations and communities that continue to build cybersecurity capabilities and capacities in developed and developing regions. This engagement provides unique insights critical to my work. I am excited at the prospect of collaborating with the Policy Impact Unit and contributing to their existing cybercrime portfolio. Understanding the real-world challenges of developing these collaborations provides rare, valuable, and pragmatic empirical evidence for both theory- and policy-relevant research contributions. On-the-ground work also provides unique perspectives into the diverse cultural and regional challenges facing Internet infrastructure development and security. These insights facilitate both impactful, responsible engagement and contribute significantly to my research-led teaching.

Research-Led Education

Understanding the social, political, and economic challenges presented by emerging trends in Internet operations, cybercrime and cybersecurity, and online platforms governance requires engaging students in contemporary, real-world problems. I am a third generation teacher—a passion and dedication to teaching is in my nature. My pedagogy uses innovative teaching methods such as flipped classroom, peer review, and intensive dialog structured to encourage respectful, yet rigorous policy debates. In my Fall 2021 course evaluations, one student wrote:

> *This is the first time I had Dr. Sowell and I felt he did a great job of explaining complex topics to a diverse audience. I was nervous to take a class without a STEM background but this class reaffirmed my decision and prepared me for other cyber courses I'm taking in the future. He genuinely cared about students learning the material and fostered critical thinking and discussion.*

Since joining the Bush School, I developed and designed, from scratch, and continue to lead and deliver, my department's Cyber Policy Concentration (CPC). The CPC is part of the Masters of International Affairs,[1] and offers a comprehensive curriculum and development programme for masters students coming from diverse disciplinary backgrounds. As part of this development programme, in addition to my own advisees, I advise students across the CPC on their course plans, and research and career objectives. This interdisciplinary, research-led programme (now in its third year) provides accessible deep dives into digital technologies and the politics and policy shaping these complex systems' design, operations, and security. I singlehandedly developed, lead, and teach four of the five courses in the CPC:

Introduction to Cyber Policy: Internet technologies foundations; longstanding issues such as attribution and encryption; contemporary issues such as privacy/surveillance and disinformation

Data Science and Visualization for Policy Analysis: exploratory data analysis (clustering, social network analysis, text mining) and visualization for mixed methods hypothesis generation

Internet Infrastructure: Platforms and Politics: deep dive into the institutional and infrastructure economics of online platforms and infrastructures

Advanced Cyber Policy: evaluates the diverse complex of institutions shaping Internet governance through the lens of political authority and a systems approach to global governance

I also lead capstones (Masters group projects) engaging with the National Cyber Forensics Training Alliance (NCFTA) and the FBI.

Over the last four years I contributed to STEaPP's teaching portfolio with guest lectures in *Risk Assessment and Governance* and *Digital Technologies and Policy*. I am familiar with STEaPP's curriculum and course structure, and would love to work with STEaPP colleagues to integrate my courses into the MPA in Digital Technologies and Policy as well as identify crossover topics with other routes. My Introduction to Cyber Policy and Data Science courses can easily be tailored as postgraduate or advanced undergraduate courses (syllabi included as supporting documents); the other two courses are appropriate for advanced MPA students and

[1] Concentrations are similar to MPA routes in STEAPP. Our two-year masters requires students to complete two (optionally three) concentrations to graduate.

can also be adapted for doctoral researchers. I am also keen to contribute to STEaPP's MPA group projects. In addition to relationships with law enforcement, I have extensive partnerships with organizations such as the Cyber Defense Alliance (CDA) and the Global Cyber Alliance (GCA), both based in London, that would be excellent partners for MPA group projects in digital technologies and policy.

I also have substantive experience with the broader dynamics of technology and policy higher education programmes. I have recently joined the advisory board for the Program on Emerging Technologies (PoET) at MIT's Political Science Department, and I have participated in and helped coordinate the Technology, Management, and Policy Consortium for graduate research into technology and policy. Through these experiences, I have engaged with colleagues and leadership from programmes such as Engineering and Public Policy (EPP) at Carnegie Melon University and the Department of Technology, Policy and Management at TU Delft. I hope to establish closer ties and collaborations with STEaPP's sibling programmes, ensuring the department continues to be competitive and on the cutting edge of technology and policy research and teaching in the years to come. In my broader service portfolio, I have served on my department's admissions committee for three years, our current department head search committee, and university-level scholarships and grant review panels, among others.

I am extremely excited at the prospect of bringing my ongoing research projects, teaching, access to expert networks, and engagement initiatives to UCL STEaPP. Please do not hesitate to contact me at jesse.sowell@gmail.com or +1 517 214 1900 with any questions about this application. Thank you for your time and interest, I am looking forward to hearing from you.

Sincerely,

Jesse H. Sowell II

February 14, 2022

Severin Walker
101 Woodcrest Rd
Suite 141
Cherry Hill, NJ 08003

Dear Faculty Search Committee,

It's my pleasure to strongly recommend Jesse Sowell for Lecturer in Science, Technology, Engineering, and Public Policy. My name is Severin Walker, and I am the Director of Provider Products and Services at Vade Secure, formerly Directory of Risk and Policy Intelligence at Comcast, with 22 years of experience in anti-abuse and cybersecurity. Additionally, I serve as the Board Chairman at the Messaging, Malware, and Mobile Anti-Abuse Working Group (M^3AAWG), a non-profit industry organization of which Comcast was a founding member.

As the M^3AAWG website states, "*The Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation. We are the largest global industry association, with more than 200 members worldwide, bringing together all the stakeholders in the online community in a confidential, open forum. We develop cooperative approaches for fighting online abuse.*" The group was initially a closed forum for operators and security researchers to discuss and collaborate on solutions for the problem of email spam. In its 17 year history, the scope of work has expanded as the problem domain of online abuse and fraudulent activity has grown and evolved. It is within this organization that I have had the opportunity to work with Jesse on multiple fronts in cybersecurity.

Nearly 6 years ago I began discussions with Jesse as I began my tenure as Chairman. He was already established as a Senior Advisor, providing valued input to our evolving efforts in global outreach and network anti-abuse initiatives, including our initial focus on the Internet of Things (IoT) and distributed denial of service attacks (DDoS). While Jesse's age and time in the industry was shorter than many of our Senior Advisors, he was provided the title given his unique status as an interdisciplinary researcher that can speak to technical, operational, policy, and organizational aspects of anti-abuse rather than one specific domain or service. This wide breadth of knowledge, as well as exposure to the members of the industry that are integral to the Internet's core functions, made Jesse a natural fit to overhaul our Outreach initiative and organizational development strategy.

While M^3AAWG itself is a global organization, with typically more than 25 countries represented at each of our 3 annual meetings, there are obvious roadblocks in many regional operators and researchers' ability to participate in person. These can be the perceived language barrier or a lack of travel budget to accomodate US or European destinations. Jesse recognized this, and the need to potentially bring resources to these regions in order to gain those additional, diverse voices in the work of M^{3}AAWG. Jesse provided the board with an entire strategy, including short and long-term goals, for consulting with regional Internet organizations to establish their own Anti-Abuse Working Groups. Starting with Latin America, Jesse joined with other M^{3}AAWG subject matter experts to introduce the idea and help establish the Latin America and Caribbean Anti-Abuse Working Group (LAC-AAWG) in 2017 through on-site collaboration in regional meetings. Per his roadmap, M^{3}AAWG now provides resources, including translated best practice documents, training, and speakers to support LAC-AAWG events hosted at these regional operator meetings. In return, LAC-AAWG members committed over a year's worth of effort as joint authors on a new Best Common Operating Procedure document on a topic of global importance, but one that was especially a priority for developing regions: in-home device security.

Still keeping with Jesse's strategy, the successful establishment of LAC-AAWG has led to work in other regions. In November of 2019, the second annual meeting of the Japan Anti-Abuse Working Group (JP-AAWG) was hosted in Tokyo with its official charter being published later that year. JP-AAWG has been going strong since. Taking many cues from M^{3}AAWG and Jesse's consultation, this has turned into a successful area of collaboration for Japanese carriers, vendors, government officials and academics in a business culture that does not typically allow for such. Jesse also worked closely with network operators in Africa to develop the Africa Anti-Abuse Working Group (AF-AAWG). AF-AAWG has now formalizing its charter in collaboration with the major operational groups in the region (AfriNIC, the regional internet registry; AfricaCERT, organizing computer emergency response teams and training across Africa; AfTLD, coordinating top level domains in Africa; and organizations representing Africa's research and education networks). Jesse will be continuing his outreach work as our liaison to AF-AAWG.

So far, since Jesse started his work on it in 2016, M^{3}AAWG has invested approximately $40,000 in support of Jesse's Outreach initiatives. Given the amount of new collaborators it has brought into our own meetings, as well as the obvious results shown in regional work, this is considered a complete success by the M^{3}AAWG board and members. Development work continues in Africa and Southeast Asia, including South Korea, with a unique approach to each as contacts in the region, M^{3}AAWG board members, and Jesse determine the needs and available resources for each.

As mentioned before, the scope of work at M^{3}AAWG has evolved to encompass several forms and vectors for online abuse and malware propagation. One that became apparent for M^{3}AAWG to consider is IoT device security and its role in Denial of Service and malware attacks. Unfortunately, while M^{3}AAWG had many of the operators represented that these devices are connected to, the rest of the supply chain, regulatory, and security research elements are not in attendance enough for many elements of the problem domain to be addressed. It was here that the board saw an opportunity for Jesse to utilize his industry resources and experience, and as such was named chair of the IoT SIG to begin steering it towards having great impact.

Shortly after taking on this responsibility, Jesse was able to bring in outside academics and industry speakers to highlight the critical role of the anti-abuse community in IoT. As someone responsible for both M^{3}AAWG's place in the industry and the protection of customers, I believe this is some of the most important work undertaken for the purposes of consumer protection and health of the Internet at large. Jesse has been able to start building a collaborative effort on the idea of a reputation mechanism that fits with ongoing ISP and industry IoT standards development efforts. In my opinion, given the unchartered waters here, this is an intelligent direction to take as it builds on some of the existing subject matter expertise and solutions built by M^{3}AAWG members and should lead to something that operators and security vendors can easily deploy given its analogues in other anti-abuse solutions in production today.

The running thread throughout all of Jesse's work with our organization is his ability to apply a deep understanding of the technologies at play in core Internet services to larger organizational and industry anti-abuse efforts. He often serves as our liaison to C-level and other high-level administrative officials to convey the work that M^{3}AAWG is undertaking and the specific contribution that their organization can make. He is a valued and sought-after advisor because of this unique quality, and would be an asset to any segment of the industry looking to facilitate collaboration for the purposes of cybersecurity and the health of the Internet in general.

If there is any need to clarify my statements here, please do not hesitate to contact me.

Sincerely,

Severin Walker
severin.walker@vadesecure.com

APWG

Unifying the Global Response to Cybercrime

Peter Cassidy
Cambridge, MA

February 14, 2022

Dear Faculty Search Committee,

It's my pleasure to strongly recommend Dr. Jesse Sowell for the position of lecturer in the Department of Science, Technology, Engineering, and Public Policy at University College London. My endorsement here is composed with some urgency as our times demand the attentions of scholars of broad expertise and the kind of acumen that can build bridges between the relevant disciplines that cyber affairs occupy by their nature.

Cybercrime arrived in the Anglophone democracies and Brazil, (of course), in the early naughts and set its sights on retail banking customers to devastating effect. Since then, cybercrime has expanded in scope and in its industrial architecture (however illicit its constituents' enterprises) and now has the power to damage key nations' economies and political stability.

Response to cybercrime with one-off legislative efforts or technical approaches or prosecutions of cybergangs or deployments of public awareness programs will always leave civilization far behind the attacking cohort and at increasing peril. Comprehensive solutions must emerge from hybridized approaches drawn from multiple disciplines and domains at once in order to be effective to any degree that matters.

This is where Dr. Sowell's scholarship is key to much more than advanced research at UCL – but to realizing the language and tools that are required to interrogate global cybercrime threats and posit solutions that would leverage the writ and purview of the intersecting institutions that must be orchestrated to actually effect those solutions.

Dr. Sowell's work came into view at Anti-Phishing Working Group (APWG) some years ago, perhaps inevitably, given the consonance of his research and APWG's mission. As a trade association, APWG's institutional motivation is to give operations and technical managers a seat at all the tables in which the work of its members could be dis-impeded - or complimented - by policies, standards or conventions of domains that intersect in its members' mission to manage cybercrime.

APWG has made its presentations and data contributions in that regard at European Commission, Council of Europe (Budapest Convention on Cybercrime), the Organization of American States, OECD, IMF, Commonwealth of Nations (Cybercrime

Initiative), United Nations (Office of Drugs and Crime), and the Organization for Security and Co-Operation in Europe. After 15 years of providing data and analyses to these treaty organizations, APWG's role seems to be shifting toward providing recommendations and prioritization criteria – tasks that would benefit from the research energies of Dr. Sowell and his students at UCL.

Further, APWG has over the years contributed commentary to these bodies as well as to key nations' ministries and engaged them as data exchange partners.[1] Most recently, APWG embarked upon a series of data policy research symposia in order to pull together the research disciplines and authoritative venues that must act in concert to effect meaningful solutions of global scale.[2]

Dr. Sowell, in fact, helped to organize our latest full-spectrum data policy symposium in Barcelona in 2018, building the agenda and bringing in a number of key investigators to the delegation adding important perspective to an already vibrant dialog that needed their voices to balance with its largely industry and law enforcement constituencies. A number of APWG industrial members pointed out that the translational nature of the dialog and the interdisciplinary approach was essential, one of which, now a recently acquired Microsoft company, is considering sponsoring another of these policy symposia in partnership with APWG.

Dr. Sowell has already been incorporated into the project planning at APWG's Applied Research Secretariat, a sponsored research section that is beginning its tenure as a research center within the larger APWG/APWG.EU plexus. Our PhishFarm project, which will measure the efficacy of browser blocklists to list and deflect users from accessing phishing websites, will engage Dr. Sowell as an analyst to consider policy aspects that the resulting PhishFarm data precipitates may illuminate. Do please note that this project is the first of any number that will follow that will be available to his MPA students and doctoral candidates in the coming years.

My sense, as a founder and Secretary General of APWG and a research collaborator to a number of university researchers in different capacities, is that Dr. Sowell's appoint-

[1] APWG Policy and Position Papers and Correspondence 2010 to 2020 (Abridged) https://ecrimeresearch.org/applied_research/

[2] https://apwg.org/2018-symposium-on-policy-impediments-to-cybercrime-data-exchange/

ment would be of enormous benefit to your research, engagement, and graduate student community with concentrations in cyber related studies directly and immediately – and, further on, as a catalyst to STEaPP's institutional development as a center of cyber research that is referenced by industry, policy, law enforcement and multilateral communities.

Dr. Sowell's experience in bridging the interests of policy communities and operational and technical cohorts is exactly what is needed today if managing cybercrime to the margins as we've done with communicable disease is to be achieved at similar global scale. Establishment and cultivation of venues (in the academy and elsewhere) that emphasize public-health models of intervention against cybercrime is key to a truly globalized response to cybercrime.

In the candidacy of Dr. Sowell, it is this correspondent's opinion that STEaPP has an opportunity to bring an innovative, outgoing researcher and lecturer into its ranks but, most importantly, to draw important communities of interest to its door and make the best use of them to ignite and maintain keystone dialogs that have yet to be fully invigorated, memorialized and codified within authoritative venues.

Among those communities of interest will be the APWG and its varied crowd of researchers, cops, policy types, industry investigators and diplomats who have gathered around the APWG's own eCrime research symposia (since 2006, with proceedings published by the IEEE) and the APWG's eCrime eXchange cybercrime data clearinghouse.

Do please know I look forward to the news of Dr. Sowell being engaged by STEaPP but the discussions I anticipate with greatest excitement are those regarding APWG and STEaPP collaborations over key questions of managing cybercrime in our time.

Regards,

Peter F Cassidy

Peter Cassidy
Secretary General
APWG

Operational Epistemic Authority in the Internet's Infrastructure

Jesse Sowell

Abstract
Internet communication increasingly intermediates our social, economic, and political lives, yet the technical communities coordinating its critical functions remain understudied. This article provides an empirical analysis of how two of the communities managing functions essential to Internet communication—addressing and routing—create the rules and operational order that sustains global communication. Analytically, this article expands the typology of epistemic authorities at play in the global governance system to include those that have accrued authority through their direct management of global, complex infrastructures. These analyses fill gaps in both the international relations and Internet governance literatures, offering a framework for systematically evaluating epistemic quality and integrity in terms of how authority is created and sustained. The article concludes with a brief analysis of how to more effectively integrate these authorities into the global governance system.

Introduction

In the 1990's, the Internet transitioned from a government experiment started in 1969 into a communications infrastructure that increasingly intermediates our social, economic, and political lives, with implications ranging from how societies share ideas, to economic growth and international security. Absent substantive government intervention and regulation, the communities of engineers and operators that manage these core functions, self-identifying as the operations community, have grown from an epistemic community of academic and industry actors contributing research and development expertise in an experimental network to transnational epistemic authorities shaping the topology, performance, and politics of the modern Internet's infrastructure. Despite their importance, the institutions and communities maintaining the functions necessary for all Internet communication—address delegation and routing—have been understudied, relegated to the low politics of technical standard setting and operations.

In the literature, the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF) are often framed as the center

doi:10.1017/xxxxxxx xxxx

of Internet governance, inspiring to van Eeten and Mueller critique this focus in their article entitled “Where is the governance in Internet governance?”[1] This article evaluates how operations communities function as epistemic authorities. One distinguishing feature of operations communities is use a bottom-up process referred to as “rough consensus”[2] to create (and maintain) the knowledge and rules necessary sustain core functions, apace with changes in the Internet’s infrastructure. Rough consensus is a means of pragmatic problem identification, evaluation, and consensus-based rule-making[3] based on operational experience.

Through two empirical cases on operations communities as epistemic authorities, this articles contributes the notions of diffuse and structured operational epistemic authorities to the broader typology of epistemic authority in the literature. Operations communities are private authorities[4] with deep, experience-based knowledge, with essential distinguishing characteristics of both Haas’s (1992) epistemic communities and Zürn’s (2018) epistemic authorities. Following Haas, these communities have distinct means of creating and validating knowledge, and an authoritative claim to that knowledge,[5] but they are not (currently) formally embedded in policy processes. Like Zürn’s epistemic authorities, operations communities are focused on impartial evaluation of their domain,[6] in this case, the security, stability, and integrity of resources critical to the Internet’s core functions. Operational epistemic authorities are valuable sources of expertise, but the source of their authority differs in two significant ways. First, their authority was not delegated by a political authority;[7] it accrued by virtue of their unique access to and management of critical resources. Second, rough consensus’ requires valid contributions be rooted in acknowledged expertise. This characteristic of rough consensus is a key factor contributing to endogenous legitimacy and sustaining these communities’ epistemic authority.

Rough consensus has embedded appropriateness values that shape the scope of operations communities’ authority. In particular, these values shape the kinds of rules made and, importantly how and under what circumstances enforcing these rules and their operational image of order may interfere with the high politics of domestic and international affairs. The values embedded are not derived from the politics of conventional transnational issues, such as human rights or economic security. Interview subjects were quick to highlight “we do not make public policy, we make [Internet] resource policy.” The rule of thumb in these communities is that rules are strictly about operations and resource policy. These values are derived from the

[1] See both van Eeten and Mueller (2013) and Hofmann, Katzenbach, and Gollatz (2017) addressing this question.

[2] Clark 1992; Russell 2006.

[3] Here, rule making is used to capture the range of rules, norms, standards, and best practices. It does not imply legal rule making.

[4] Hall and Biersteker 2003; Büthe and Mattli 2011.

[5] Haas 1992, 2-4.

[6] Zürn 2018, 51-53.

[7] And as elaborated later in this article, cannot be easily rescinded by political authorities.

politics of operational efficiency rooted in the custodianship of (common) resources that contributing to the integrity of Internet communication.

This article contributes analyses of the history and function of these epistemic authorities and their relationship to Internet governance and the broader global governance system. It then builds on these empirical cases to expand the typology of epistemic authority. First, this article disentangles the function and objectives of operations communities from broader communities engaged in more public facing elements of the infrastructure (namely the domain name system, coordinated by ICANN). Given these foundations, the notion of *operational* epistemic authorities is presented relative to existing theory, then in the context of its foundations in the early experimental Internet, ultimately leading up to the formation of the modern institutions in which rough consensus serves to ensure credible knowledge assessment and the development of rules that keep pace with growth and technological change. Rough consensus itself is then presented as an adaptive, reflexive[8] rule making process, couched in how values rooted in operational efficiency are embedded in the process and shape these authorities image of liberal order. This article concludes by returning to the question of impartiality and legitimacy in this emerging form of epistemic authority, for both the Internet, and more generally for a society with increasing dependence on complex, decentralized infrastructures for which expertise, and resource provisioning and management, are embedded in distinctly transnational epistemic authorities.

Delving *in*to the Internet's Operations Communities

Colloquial notions of "the Internet"[9] include a broad set of activities: activities facilitated by applications such as e-mail, activities on platforms such as Facebook, and, most salient here, those unseen activities playing out in the supporting infrastructure. Solum (2008) notes that

> If the topic of Internet governance were taken as the investigation of the regulation of all the[] activities [that take] place on (or were significantly affected by) the Internet, then 'Internet governance' would be more or less equivalent to 'law and politics'.[10]

Broad framings of Internet governance confound the loci the diverse governance regimes at play and their spheres of authority. Platforms such as Meta's social media platform Facebook and online shopping platforms such as Amazon Marketplace are built *on* the Internet, relying on its infrastructure for global connectivity. They are

[8] Scott 2015; Black 2017; Sabel, Herrigel, and Kristensen 2018; Zürn 2018, Chapter 2.

[9] See Abbate (2017) and Haigh, Russell, and Dutton (2015) for discussions on the framing what is precisely meant by "the Internet" and the scope of activities entailed in those framings.

[10] Solum 2008, 49.

(thus far[11]) largely regulated and governed by those multinational firms, according to their interests. In contrast, common resources critical to the function of the Internet's infrastructure—here in particular addresses and routes—are managed by globally diverse, transnational communities *in* the Internet's infrastructure. This distinction between governance "in" versus governance "on" offers a first, coarse-grained cut at the spheres of authority at play, and how their modes of governance differ.

The "Internet governance" literature has focused on the social construction of Internet protocols vis à vis law and policy in the Internet Engineering Task Force (IETF);[12] and on ICANN and the IGF as the loci of governance and policy engagement.[13] van Eeten and Mueller (2013) rightly critique this latter, highlighting a much greater diversity of issues such as privacy, censorship, intellectual property, and security, to name a few.[14] In this literature, the operations communities, in particular those managing address delegation and routing, are often grouped alongside ICANN for completeness, but their modes of rule-making, governance, and authority are not elaborated.[15] Based on engagement through interviews and fieldwork, these communities explicitly distinguish themselves from the ICANN and IGF communities, and those managing familiar activities on platforms such as Facebook.

While not as visible as ICANN and the IGF, operations communities are not hard to access. These communities pride themselves on the openness of their meetings to anyone willing to engage and learn. That said, technical and operational knowledge is a barrier to entry for fieldwork in these understudied communities, and for these communities' engagement in the global governance system. This knowledge is necessary to understand the nuance of the topics de jure, why they are important, and their implications. It is also necessary to understand why rough consensus, as a mode of credible knowledge assessment, is fit to purpose for rule-making in this dynamic sociotechnical environment. An early interview subject rightly highlighted that simply *reading* about these processes is very different from observing the diverse, critical dialogue among participants firsthand.

The empirical work supporting this article builds on archival analysis of operational (resource) policy documents, e-mail lists (live and archived), and ten years of fieldwork and interviews with over 100 actors from globally diverse operations communities. Archival analyses include textual analysis of e-mail lists, online archives of resource coordination policies (rules produced by these communities), and documentation of resource policy development processes themselves (the ways these rules are created).

[11] These platforms have seen increasing scrutiny from domestic and international policy makers; their governance has also been implicated in the contention between illiberal states and the liberal international information order (Farrell and Newman 2021).

[12] Braman 2010, 2011, 2013; DeNardis 2009.

[13] Mueller 2002; Klein 2002; Take 2012; Raymond and DeNardis 2015; Becker 2019; Jongen and Scholte 2021.

[14] van Eeten and Mueller 2013, 723.

[15] There are mentions of what they do, and broader discussions of Internet governance citing the efficiency of private governance writ broadly, but little evaluation of precisely how or why.

Much of the engagement in these communities occurs in regional and global meetings. Supplementing these face-to-face meetings, operations communities use e-mail lists to discuss common issues, facilitate broader community participation, and as a (partial) archive of policy discussions. Active e-mail lists (and the corresponding archives) were starting points for understanding community dynamics, for identifying meetings for fieldwork, for identifying substantive issue domains, and for identifying participants for semi-structured interviews.

Interview subject selection criteria included:

1. longstanding *and* relatively new community participants;
2. frequent authors of operational policy proposals and frequent contributors to policy dialogues (later differentiating between frequency and quality of contribution, as in the rough consensus process itself);
3. actors in formal and informal leadership roles;
4. actors from different technical interest groups, and Internet infrastructure subindustries, and
5. actors from employers of different sizes and geographic scope.

Snowball sampling[16] further contributed to the scope and diversity of participants necessary for content validation.

Two categories of prompts were used to explore participants' experiences. The first focused on validating rough consensus as a process. The second focused on the strengths and limitations of rough consensus. In particular, these prompts focused on rough consensus as a form of credible knowledge assessment fit to the purpose of making rules in a sociotechnical environment and sustaining epistemic authority. Interviews integrated information collected from archival analysis, fieldwork, and previous interviews to cross-validate events and processes, comparing and contrasting perspectives and expert opinions on the norms, best practices, and resource policies discussed.

Process tracing[17] was used to systematically evaluate how rough consensus contributed to rule-making and sustaining epistemic authority. In particular, process tracing was used to validate the black letter of formally documented rough consensus processes relative to participants' experiences and observations of the process, and to identify differences across organizations. Fieldwork, interviews, and comparative analysis contributed to the detailed evaluation of rough consensus and understanding the epistemic community's political culture, in particular its aspirations to limit the scope and impact of its activities (these communities' sphere of authority) to operational rule making. Placing these in their historical context highlights the distinctly path dependent[18] character of how authority gradually accrued and is sustained. This process also highlighted how rough consensus contributes to self-

[16] TenHouten 2017; Noy 2008.

[17] George and Bennett 2005; Bennett and Checkel 2015.

[18] David 2007.

reinforcing feedback.[19]

Simple, Generative, and Liberal

Writ narrowly, the Internet (as an infrastructure) has one intentionally simple, yet highly adaptive, general-purpose function: move data from here to there.[20] The simple functions described in this section—addresses to uniquely identify devices and routing data across the Internet from one device to another—are necessary for *all* Internet-based communication: checking one's e-mail, interacting with web pages and social media, streaming the latest episode of your favorite series, secure online banking . . . the list goes on and on. From an infrastructure economics perspective, the infrastructure is an essential common factor of production contributing to the diverse (downstream) "public, private, and social goods"[21] built on Internet communication technologies.

The function itself is simple; the collaboration necessary for ensuring security and stability is a complex sociotechnical process. This section describes these functions and the role of the operations community sustaining those functions. It then argues how the general-purpose (generative) character of these functions' contribute to the liberal character often attributed to the Internet, and the role of the operations community in sustaining that liberal character.

Simple Function

Jon Postel, an Internet pioneer that coordinated common resources critical to early inter-networks that would become the Internet, concisely summarized the role and function of these resources:

> A *[domain] name* indicates what we seek. An *address* indicates where it is. A *route* indicates how to get there.[22]

Domain names such as *facebook.com*, *amazon.com*, and *gmail.com* are the most visible. Domain names (in community vernacular, simply *names*) were initially created to add semantically meaningful labels to seemingly meaningless numeric addresses; governance and regulation of the domain name system (DNS), often focusing on ICANN, has been studied quite extensively.[23] Names have become integral to the

[19] rixen2016historical

[20] For the design principle behind this simple function (the end-to-end principle), see Saltzer, Reed, and Clark (1984) and Blumenthal and Clark (2001). For an analysis of differing interpretations, see van Schewick (2010).

[21] See Frischmann (2012) for discussion of infrastructure as a common factor of production for a wide variety of public, private, and social goods.

[22] Emphasis added here. Famously attributed to Postel (1981, 7), paraphrasing Shoch (1978, 1).

[23] The most well known work on the domain name system (DNS) is Mueller (2002). See also X

behaviors and features users expect in platforms, but are not essential to the Internet's core function. In contrast, addresses and routes provide the information necessary for data to get from here to there; without them, there would be nothing to give a meaningful name to.

Addresses uniquely identify devices such as laptops, tablets, mobile phones, the increasingly broad array of "smart" IoT devices, and importantly, the networking equipment along the paths (routes) necessary to move data from one device's home network, through intermediary networks, and on to the destination device's network (for instance, from an academic's laptop to the server hosting an article submission platform). It would be inconvenient not to use domain names, but the data would still get there. Consider a simple analogy. The proper name of a place, such as the Museum of Modern Art (MoMA) in New York City, tells one what kind of place it is and a bit about what they will find there. Without the address and an authoritative map one can use to identify the most efficient route amongst a variety of possible paths, modes of transport, and considering neighborhoods and congestion, it would be very difficult to get from, say, one's home or office, to the MoMA. The name is convenient and useful, but the addresses and routes are essential.

Following the MoMA analogy, there are multiple routes, over multiple modes of ground transport—walking, subway, bus, personal vehicle—that one can select from. In the Internet, there are also many routes to choose from, some more desirable than others.[24] With the exception of frustrating construction on the ground, the map of New York City (and that of physical, resource intensive infrastructures in general) is relatively static. In contrast, the map of the Internet, i.e. the collection of all possible routes, is constantly changing, dynamically, on a near continuous basis. Routes change for various reasons: changes in contractual relationships between networks, outages,topological changes (new physical infrastructure, such as fiber optic cables in the ground or submarine cables), to improve performance, or for economic and national security[25] reasons. Coordinating across one hundred thousand plus networks[26] creates endemic, unavoidable uncertainties, requiring human intervention and rules to maintain consistent function, a form of operational order.

Adding to this complexity is that, on the technical side, this map is drawn and maintained using a protocol colloquially referred to as "routing by rumor."[27] Networks

[24] Of the many routes available, some are longer (take more time), some are less stable (data is lost, meaning it has to be resent, potentially affecting the performance of applications like video streaming), and for security purposes, it is often considered undesirable to route traffic through jurisdictions known to monitor Internet traffic.

[25] For instanced, routing to avoid jurisdictions known to monitor Internet traffic, or to ensure local, sensitive traffic stays local.

[26] Calculated based on the number of autonomous systems in the Internet, as reported by the Number Resource Organization (2022).

[27] The protocol for distributing routing information, the Border Gateway Protocol (BGP) (Rekhter (Ed.), Li (Ed.), and Hares (Ed.) 2006), is a distance vector algorithm referred to colloquially in the community as "routing by rumor." Among the operational epistemic communities discussed here, this colloquialism is

"advertise" to their neighbors the addresses in their networks, and the information about the routes *through* their networks they are willing to make available to get to other networks. Those neighbors incorporate that routing information into what they know from *their* neighbors, update their own advertisements, and advertise onwards. In effect, the map of the Internet is updated based on the continuous chatter between networks about what routes are available, which have changed, and which have been rescinded. Like all chatter and rumors, it is best to confirm what one hears from an authoritative source, but that is a transaction cost for networks, just as it is for individuals. "Routing by rumor," was initially developed when routing chatter was exchanged in a community of a few hundred known, trusted peers. It is still effective today, but to ensure consistent, stable routes, in addition to the flexibility baked into Internet protocols, operations communities also developed norms, best practices, and resource policies to mitigate and remediate negative network externalities when rumors turn out to be false.

A well known adage illustrating the operational order in addressing and routing is that "the Internet interprets censorship as damage and routes around it."[28] The incident between Pakistan and YouTube in 2008, over blocking a video offensive to the Prophet Mohammad (illegal in Pakistan), illustrates the implications of routing by rumor and how these actors resolve network externalities. When YouTube refused Pakistan's request to take down the video, Pakistan attempted to manipulate *local* routes to redirect Pakistani traffic intended for YouTube to a local destination, managed by the Pakistan Telecommunication Authority (PTA), that indicated YouTube was hosting illegal content. When Pakistan implemented their intervention, not only were local YouTube users in Pakistan redirected to the PTA's website, but users *around the world* were redirected. From the perspective of the operations communities, Pakistan had "hijacked" YouTube's addresses, violating routing norms and contractually binding address policy, resulting in damage to the integrity of the Internet's routing system. Operators around the world identified the "damage", shared what they knew about the "illegitimate" route advertisements within the community (across firm and jurisdictional boundaries), and began correcting their own routing advertisements to ensure traffic intended for YouTube's addresses did in fact get directed to YouTube's servers. This global network externality between Pakistan, YouTube, and the transnational network of Internet operators played out, and was resolved, in approximately three hours.[29]

The Pakistan-YouTube incident illustrates more than just technical mechanics. First, it illustrates one of the operations community's core images of *order*: accurate

frequently used in explaining the nuance of BGP. More recently, it is also used to explain some vulnerabilities, calling for more secure (cryptographically signed) announcements of routing information akin to officially signed letters than rumors.

[28] John Gilmore, quoted by Elmer-DeWitt and Jackson (1993).

[29] The RIPE NCC produced an excellent video (now on YouTube) (RIPE NCC 2008) illustrating precisely how this happened.

distribution of routing information. Second, it illustrates the *capabilities and capacities* of the operations community to correct damage and maintain their image of operational order. Third, it illustrates the *willingness* to use these capabilities and capacities to maintain its image of operational order. Finally, it demonstrates one end of the spectrum of operational epistemic authority developed here: diffuse authority, applied by a "close-knit yet loosely organized" community when its norms were violated. These characteristics of the operations community are not only important for maintaining operational order, but enforcing these norms is also one of the ways the liberal character of the Internet's infrastructure is maintained.

Generative and Liberal

These core functions and the associated rules are also important for understanding the liberal character of the Internet, frequently attributed to the open, free flow of information.[30] Zittrain offers the notion of generativity as "a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility."[31] The generative character of the Internet rests on *(1)* the programmable personal computer (PC) and, important here, *(2)* the Internet's simple, general purpose communications protocol (the Internet Protocol, IP). Used in conjunction with one another, these complementary technologies not only drastically lowered the barriers to transnational engagement, but also lowered the barriers for developing tools and platforms that cultivate and sustain transnational polities.[32] In *Inventing the Internet,* Abbate highlights that when the early ARPANet was primarily used for sharing access to geographically distributed computing resources and data among researchers, it was under utilized. Utilization increased substantively with the use of e-mail, highlighting the Internet's potential for catalyzing human collaboration.[33]

The generative character of the Internet opened the door to developing the diversity of interactive platforms that make up today's Internet. This same generative potential also facilitates many of the malicious activities, such as spyware and ransomware. In this sense, it is liberal, to an extreme. Absent significant regulatory order *on* the Internet, it is arguably liberal to a fault. Any set of actors, regardless of their normative intent, liberal or illiberal, can collaborate to create innovative online tools and platforms, for licit or illicit purposes. Consider two contemporary instances. Social media platforms range from mainstream platforms such as Facebook to "alternative" platforms such as Parler. As another instance, platforms have been developed to facilitate engagement in legitimate electoral processes, and malicious actors have developed platforms commoditizing disinformation campaigns intended to distort

[30] Farrell and Newman 2021.
[31] Zittrain 2006, 1981.
[32] Nye and Keohane 1971.
[33] Abbate 2000, 105-112.

democratic processes.

Although the epistemic authorities maintaining the Internet's infrastructure do not use the term generativity, maintaining the (liberal) general purpose character of Internet communication, and the innovation attributed to this design,[34] has become, in and of itself, a normative ideal. Particularistic governance issues (such as what constitutes abusive messaging, or what constitutes disinformation on a given platform or in a given jurisdiction) are considered the domain of public authorities and/or the managers of platforms built on the Internet. This latter distinction highlights two coarse-grained spheres of authority in the global governance of Internet-related activities: those ensuring the general-purpose character of simple communication *in* the Internet's infrastructure and those regulating the particularistic behaviors that play out *on* the Internet. As illustrated by the two contemporary instances above, these latter intersect directly with conventional domestic and transnational policy and security issues.

This distinction is also critical for understanding the scope of private Internet governance often cited in the literature. Consider Farrell and Newman's argument that attributes self-undermining contestation in the liberal international information order (LIIO) to openness and private-actor governance, citing activities motivated by "data-driven advertising" and "[n]ew media ecosystems, driven by the imperative to maximize 'engagement,' [that] favor[] controversial fringe material while offering opportunities for political entrepreneurs to exploit and widen fissures in political knowledge."[35] The argument certainly holds, but it is important to note that, in this case, self-undermining contestation, as characterized above, is a consequence of private governance of platforms developed by individual multinational firms managing social media platforms *on* the Internet, that, relative to the general-purpose character of the Internet's infrastructure, have rather particularistic goals and values shaped by the objectives of the firm (such as Meta) or the politics of a particular group (such as Parler). In contrast, distinctly pluralistic, transnational epistemic authorities *in* the Internet focus on sustaining its simple communication function, and the general-purpose (generative) character of that function. First, embedding particularistic values would limit the general-purpose function, foreclosing on a number of real and potential downstream uses.[36] Second, interviews indicate that it is not in these actors political or economic interest to limit the general-purpose character or (unnecessarily) interfere with transnational issues playing out atop the Internet *unless* those actions interfere with the integrity of the infrastructure itself (viz. Pakistan-YouTube). Rather, those issues fall more appropriately within the spheres of authority of domestic and international policy makers and regulators.

The operational epistemic authority illustrated in the Pakistan-YouTube case is

[34] See van Schewick for one of the most complete analyses of innovation and the Internet's architecture.

[35] Farrell and Newman 2021, 341.

[36] It also runs against the fundamental design principles in the end-to-end principle (Saltzer, Reed, and Clark 1984; van Schewick 2010).

interesting because it is not delegated in the sense of Zürn's politically assigned epistemic authorities.[37] Rather, epistemic authority accrued to these communities as they grew and matured, alongside the Internet itself, in an emerging age of postnational liberalism.[38] This epistemic authority was not actively cultivated as political authority, either. Adhering to the extreme liberal character resulting from normative focus on preserving the general-purpose (generative) character of communication *in* the infrastructure means the community is extremely reluctant to hew to political objectives. Some of these kinds of actions, that do have consequences for conventional political activities and align with normative notions of liberalism[39], are often celebrated by civil society and activist organizations. These latter have imbued the Internet with these ideals, but, as a diffuse form of operational epistemic authority, they were not directed by any particular state or conventional liberal international organization. For the operations community, this was a normative imperative to restore the integrity of the (routing) system as a common good critical to the integrity of Internet communication and their value propositions.

The operational epistemic authorities discussed here vary in the formality of rule making and institutional structure. At one end of the spectrum are the routing communities, an instance of "close-knit yet loosely organized" (diffuse) operational epistemic authorities. At the other end of the spectrum is the addressing communities, an instance of structured operational epistemic authorities, which have developed formal institutional constructs comprising non-profits coordinating address delegations and transfers, documenting the rules ordering those resource management activities, and facilitating rule-making processes. The next section first contextualizes this distinctly operational mode of epistemic authority in the global governance literature, then traces how this authority emerged from the early organization and development of the Internet as an experiment through its modernization and development of resource management institutions in the late 1990s.

Operational Epistemic Authorities *in* the Internet

Epistemic communities are increasingly critical to the management of complex global infrastructures, here in particular the Internet. Private authorities are characterized as more efficient than their public counterparts,[40] but also less transparent[41] and face potential legitimacy issues.[42] In contrast to the closed private authorities evaluated by Büthe and Mattli (2011), these communities are adamantly open, actively encouraging new participants willing to learn. Like those authorities evaluated by Büthe and

[37] Zürn 2018, 51-52.

[38] Börzel and Zürn 2021.

[39] See Lake, Martin, and Risse (2021, 229-232) for a recent typology of the kinds of liberalism.

[40] Cutler, Haufler, and Porter 1999; Hall and Biersteker 2003.

[41] Mattli and Büthe 2003; Büthe and Mattli 2011.

[42] Underhill and Zhang 2008; Zürn 2018.

Mattli (2011), technical knowledge and vernacular used in those communities is a high barrier to entry.

This section first defines diffuse and structured operational epistemic authorities relative to the literature, then evaluates how operations communities transitioned from research and development contractors in a small experimental Internet into transnational authorities managing resources critical to a global infrastructure. The historical context is critical to distinguishing between authority that has been politically delegated (and as such, can be rescinded) and authority accrued by these communities, intrinsic in their capabilities and capacities, and that is sustained by their ongoing operational practices and rule-making through rough consensus.

Sources of Epistemic Authority

As an epistemic community, operations communities "share[] ... normative and principled beliefs" regarding the integrity of Internet communication, have refined their notion of rough consensus as a means of "shar[ing] causal beliefs" based on experience managing the system, use constructive conflict within the rough consensus process as a "shared [image] of validity," and have the general-purpose operational integrity of the Internet as both "a common policy enterprise" and a bound on the scope of that policy enterprise (infrastructure management, minimal interference with public policy and authority).[43] Typically framed as offering expert advice, epistemic communities help domestic and international policy makers navigate complex domains or issue areas, potentially influencing broader international politics as they become more embedded in the policy process.[44] Under this framing, epistemic communities are sources knowledge salient to policy makers, but not necessarily managers of resources in the domain or issue-area.[45] In contrast, operations communities base their knowledge on direct experience coordinating a complex, global Internet infrastructure. Their knowledge base is more akin to the teleological experimental methods that characterized early engineering science than methods attributed to more traditional scientific communities.[46]

Zürn's characterization of epistemic authorities focuses on the role of these communities' "expert knowledge and impartiality,"[47] highlighting the idea of "pure epistemic authorities ... [e]specially transnational civil society organizations."[48]

[43] Quoted text from Haas's definition of epistemic communities (1992, 3).

[44] Haas 1992, 4.

[45] Haas 1992.

[46] This follows Haas (1992, 3, footnote 4). In terms of their operational knowledge of the address and routing system as a commonly managed resource, their knowledge base is developed similar to Ostrom's common pool resource managers (1990, p). In terms of the way they perform experiments, their (resource) policy experiments are akin to those described by Moss (2004). For the teleological methods of improving performance used by early engineering scientists, see Layton (1979).

[47] Zürn 2018, 51.

[48] 52.

Communities become what Zürn refers to as politically assigned epistemic authorities (PAEAs) when "assigned that status by other authorities,"[49] typically by political authorities. In this framing, "they do not make binding decisions, but [are delegated] competences to make often very consequential interpretations."[50] Here, demand for these epistemic communities' knowledge led to explicit delegations of authority that can also be rescinded based on politics or performance.

Rather than being placed "in" authority by an existing political authority, the role of operations communities as "an" authority accrued over time, as a consequence of their role and experience developing, deploying, and maintaining a functioning, increasingly complex, global infrastructure. Here, "in" authority and "an" authority are used in the sense developed by Flathman (1980, 16-19).[51] To be "in" authority is by virtue of holding an office; it is delegated and can be rescinded. To be "an" authority is "based on, is possessed by virtue of, demonstrated knowledge, skill, or expertise concerning a subject matter or activity."[52] Operations communities' collective knowledge, capabilities, and capacities developed first in regional networks that made up the early Internet (for instance, in the United States and Canada, in Western Europe, and in developed economies in the Asia Pacific). These regional communities integrated into a global community[53] as transnational demand for improved performance and capacity led to a more dense mesh of network relationships.[54] In the 1990's, the increased importance of Internet communication led to explicit demand for institutions[55] and organizations for maintaining operational order, here in particular the regional Internet registry system as an instance of structured operational epistemic authority.

The two forms of operational epistemic authorities developed here, diffuse and structured, are two ends of a larger spectrum of epistemic authorities managing technologies and operations in the Internet's infrastructure. *Diffuse operational epistemic authorities (DOEAs)* are informally organized institutions whose participants are "close-knit, yet loosely organized"[56] There is no single, authoritative source of norms and best practices; knowledge is generated largely through experience. In the routing community, knowledge is shared among peers in fora such as network operator groups (NOGs, discussed later in this section), RIR meetings, among others. Their shared causal belief and shared image of validity follows the spirit of rough consensus:

[49] 51.

[50] 52.

[51] Sea also Lake's notion of relational authority (2009).

[52] Flathman 1980, 16.

[53] Operations communities are surprisingly granular. In countries such as the US, regional operator groups are quite active. Globally, there are typically operator groups corresponding to most economies with significant Internet presence.

[54] In this case, greater capacity means greater bandwidth and interconnection relationships that reduced inefficiencies as more traffic flowed over a denser mesh of connections between countries. This latter density means more efficient paths, not necessarily more direct bilateral connections.

[55] Mattli and Woods 2009.

[56] In the sense of Ellickson (1991).

it must be based on pragmatic experience and demonstrated (performed) expertise.

Structured operational epistemic authorities (SOEAs) are rooted in formal organizations that manage or coordinate resources critical to system function and serve as the loci of rule-making (here, organizations that facilitate rough consensus). Like DOEAs, the validity of rule-making requires credible contributions by participants the community recognizes "an" authority. The organizations in SOEAs provide the fora in which these rules are made; manage resources based on the rules developed by the community; and manage the authoritative repository of the documentation of rule-making proceedings and the resulting rules themselves. SOEA organizations also play an important role ensuring the integrity of "an" authority-based rule-making procedures. It is in this process validation role that SOEA organizations are instances of those "in" authority, but those actors must be "an" authority to effectively fulfill these roles.

Accruing Epistemic Authority: From Research Contracts to Institutions

The initial Internet experiment was funded by the United States' Department of Defense's (DoD) Advanced Research Projects Agency (ARPA) and coordinated by the Information Processing Techniques Office (IPTO). The DoD contracted academics and industry actors for research and development of a decentralized, heterogeneous network-of-networks more resilient than the centralized architecture of the telephone system.

> We wanted to have a common protocol and a common address space so that you couldn't tell, to first order, that you were actually talking through all these different kinds of nets. That was the principal target of the Internet protocols.[57]

Abbate highlights that the DoD was largely a coordinator, leaving much of the development and decision making to those doing the work.[58]

> IPTO managers preferred to take the informal approach whenever possible. Having been researchers themselves, they subscribed to the view that the best way to get results in basic research was to find talented people and give them room to work as they saw fit. *They also tended to believe that differences of opinion could be debated rationally by the parties involved and decided on their technical merits, and that they, as IPTO managers, would need to intervene with an executive decision only if the contractors could not resolve differences among themselves.*[59]

[57] Vint Cerf, one of the fathers of the Internet and directly involved in its early development, quoted by Abbate (2000, 128).

[58] Abbate 2000, 54-60.

[59] 55, emphasis added.

These function- and operations-specific groups evolved into the working group structure of the IETF, the organization that currently manages develops core Internet standards and protocols.

As the Internet grew from a distributed lab experiment hosted largely at academic institutions, into an experimental government network, and on into the modern commercial Internet in the mid-1990s, the IETF emerged as the organization coordinating and documenting the development of Internet protocols.[60] In the course of these transitions, the IETF formalized its protocol standards development processes,[61] developing a variant of consensus-based decision-making common to technical standards development processes.[62] At this time, the epistemic communities convening at the IETF performed many of the functions necessary for Internet development and operations: managing and contracting physical infrastructure; development and implementation of communications protocols; developing naming, addressing, and routing standards and related protocols; delegation of corresponding resources as needed; and development of protocols underpinning common applications such as e-mail (along with a plethora of attendant security standards). Norms encouraging experimentation with implementations, and how rules and best practices were made, were not only encouraged, but necessary. These norms carried through from the relationship between early management and contractors, later under the coordination of the National Science Foundation (NSF), and ultimately into the private operations communities that took up stewardship of operations related to names, addresses, and routing, as the IETF increasingly focused on standards and protocols. Hearkening to their origins in the IETF, the operations communities, here in particular addressing and routing focused, on epistemic quality, through norms that encouraged operations and policy experiments.

As the importance of Internet communication became more broadly understood, other standards for creating "Internets" came into competition with IETF standards. Competition with another standards process gave rise to the mantra of "rough consensus and running code" that has come to characterize the ethos, and the mode of authority, in the IETF and operations communities. In 1977, the International Standards Organization (ISO) began developing an the Open Systems Interconnection (OSI) model, "to set the ground rules for network interconnection,"[63] an alternative to the IETF's TCP/IP (Transmission Control Protocol/Internet Protocol). Russell documents the standards culture war that ensued, highlighting a key point of contention: the distinct differences in the organizational structure and perceptions of authority in the IETF and ISO. According to Russell, ISO's organizational culture "resembled contemporary democratic bodies insofar as it featured voting, partisan compromises,

[60] For detailed histories, see Abbate (2000) and Hafner and Lyon (1999).

[61] Resnick 2014.

[62] See Yates and Murphy (2019), in particular Chapter 7.

[63] Russell 2006, 52.

and rule-making behavior designed to protect financial interests."[64] Russell goes on to describe that early Internet pioneers' (participants in the IETF) distaste

> stemmed from their frustration with the technical aspects of OSI as well as with ISO as a bureaucratic entity. Where TCP/IP was developed through continual experimentation in a fluid organizational setting, Internet engineers viewed OSI committees as overly bureaucratic and out of touch with existing networks and computers.[65]

In 1992, the IETF's leadership, the Internet Architecture Board (IAB), developed a draft proposal to replace IP addresses with an addressing model from the OSI model. IETF participants rebelled against the idea that the IAB was acting "in" authority, requiring the IAB to "relent . . . in the face of a massive 'palace revolt'."[66] The IAB did relent, and in doing so clarified the ethos of standards development in the IETF, and its way of evaluating knowledge and resource policies in the emerging operational epistemic authorities.

In a presentation responding to this revolt, Dave Clark presented a clear and distinct articulation of this ethos, now part of the IETF's mission statement.[67]

> We reject: kings, presidents, and voting. We believe in: rough consensus and running code.[68]

It is important to be clear that this is not intended as a rejection of government authority writ broadly, but a statement about the kind of authority that characterizes the IETF. It is a reaffirmation that, within this community, there is no set of actors "in" authority that can override the epistemic consensus of the community, arrived at by credible "an" authorities. Flathman indicates "[t]hose who have such authority [(an authority)] issue statements or propositions about the subject matter, or *perform the activity in question*—statements and *performances* that allegedly have such qualities as truth, *correctness, validity*, profundity, exceptional grace or beauty, and so forth."[69] For the IETF, "running code" is that performance, rooted in correctness and validity that has been evaluated through rough consensus among "an" authorities. Documentation of these processes and in IETF RFCs are the means by which these evaluations become authoritative.

Moreover, it highlights that majoritarian voting, and the politics and vote trading that come along with this model of decision-making,[70] are inappropriate for developing protocols, standards, and operational policies that require high levels of collaboration,

[64] Russell 2006, 53.
[65] 53.
[66] 55.
[67] Alvestrand 2004, 2.
[68] Clark 1992, Slide 19.
[69] Flathman 1980, 16, emphasis added here.
[70] Lijphart 1999.

among actors considered "an" authorities. In the absence of a central governing body, for these be authoritative, they require rigorous knowledge assessment to be considered both credible and actionable (they will yield stable, running code) and rough (but not necessarily complete) consensus. This teleological perspective is also embedded in the modern operations communities' "rough consensus" processes[71]: developing norms, best practices, standards, and policies on an experimental, best effort basis, by an epistemic community that prefers developing rules based on operational experience, and evaluating outcomes (experiments, running code that yields functional, stable systems). The debates within these communities are rigorous and contentious, requiring deep knowledge of the topic at hand. If a participant cannot justify the rationale for contesting a solution in terms of empirical evidence, in reference to existing community knowledge of the system, and/or existing best practices, their contestations are dismissed. If a participant makes a regular habit of making these kinds of contestations, their status as "an" authority diminishes. Former prestige as "an" authority and former accomplishments does foster some tolerance, but if these actors engage in invalid or incredible contestations, those contestations will be dismissed as well.

Early in the development of these communities, a common objective was Internet stability; today, it is coordinating rule-making and maintaining system integrity. With the approach of the NSF's divestiture of Internet management to the private sector in the 1990s (made official in 1998), demand emerged for new *operational* coordination institutions. Two functionally related, but organizationally different, groups of operational institutions emerged to fill these gaps. The global set of network operator groups (NOGs) emerged as convening fora for the routing community, an instance of diffuse operational epistemic authority. The regional Internet registry (RIR) system emerged as a structured operational epistemic authority managing the delegation of (IP) addresses.

Diffuse Operational Epistemic Authority: Routing and Network Operator Groups

In the mid-1990s the routing community developed network operator groups (NOGs) as fora in which actors could discuss operational issues critical to ensuring global connectivity, i.e. ensuring an increasingly global network-of-networks remained glued together in a secure and stable way. Although operations communities, here in particular the routing and address communities have substantive overlap in participants,

[71] This *kind* of consensus has been in play in scientific and technical standards making since at least 1880 (Yates and Murphy 2019, 4, Chapter 1). *Rough* consensus was coined in a presentation at the IETF by David Clark (Clark 1992) (currently a Research Scientist at MIT's Computer Science and Artificial Intelligence Lab (CSAIL), and formerly Chief Protocol Architect and chair of the Internet Activities Board from 1981-1989). Russell (2006) offers a historical analysis of this term in the context of the Internet-ISO Standards War.

within these, actors make clear conceptual distinctions between the roles in, and knowledge created in those roles, in each function-specific community. In their role coordinating routing and interconnection, actors refer to themselves as the routing community, differentiating from roles in other function-specific communities such as those managing names (the DNS or naming community) or addresses (the numbers[72] or addressing community).

One of the first of these communities, the North American Network Operator Group (NANOG) was created expressly for the purpose of filling the coordination gap left by the NSF: to facilitate sharing operational interconnection information necessary to sustain global connectivity during and after the transition of coordination by the NSF to the private sector. Today, there are more than fifty network operator groups[73] around the world.[74] These range from global communities such as NANOG; to regional groups, such as LACNOG (Latin America and Caribbean), AFNOG (Africa), and MENOG (Middle East); to economy specific NOGs such as JANOG (Japan), ghNOG (the Ghambia), ArNOG (Argentina), and DENOG (Germany).

NOGs serve three primary knowledge sharing and coordination functions: sharing information and best practices about interconnection operations; supporting engagement among actors coordinating interconnection and routing between networks; and developing the relationships necessary to quickly and efficaciously mitigate and remediate network externalities. For instance, NANOG's mission highlights that it facilitates discussion among experts on topics such as "experiences with new protocols and backbone technologies, implications of routing policies on the Internet as a whole, measurement techniques and measurements of Internet health and performance, areas in which inter-provider cooperation can be mutually beneficial (such as NOC [network operations center] coordination or security incident response), and maintaining a competitive and level business environment."[75] Their bylaws go on to indicate that all presentations and tutorials are "reviewed in advance and are limited to those entirely of a general technical nature, *explicitly prohibiting material that relates to any specific product or service offerings*."[76] Within these fora, commercial presentations, i.e. marketing, is often banned, or strongly discouraged. Program review committees enforce these norms. When presenters deviate from these norms, the audience is not shy about sustaining epistemic quality, calling out the presenters (and the NOG). NOGs are convening fora for the routing community as a DOEA and many provide archives

[72] As a resource, addresses are important, but conceptually quite simple. The address community often refer to them as simply "numbers". The primary address range in use, IPv4 addresses, range from 1 to $2^{32} - 1$. In their simplest form, they are a range of integers, numbers, for used for uniquely identifying devices. The function is simple; management of delegations to networks is where the cooperation and coordination problems become more complex.

[73] Typically referred to NOGs; some are referred to as network operator forums, such as UKNOF in the United Kingdom.

[74] Greene 2021.

[75] NANOG 2020.

[76] NANOG 2020, emphasis added here.

of presentations, some of which describe best practices. That said, NOGs do not present themselves as coordinated, authoritative sources or archives of authoritative, formally agreed upon norms and best practices.

The second primary function of the NOGs is to serve as meeting places for expert network representatives[77] to engage in negotiating, establishing, and maintaining interconnection relationships between networks.[78] These contractual relationships determine which routes are shared, and with whom. These relationships range from those focused on moving traffic from one network to another to those in which a provider guarantees its clients connectivity to the global Internet.[79] The continuous process of redrawing the "map" of the Internet is a combination of these contractual dynamics and "routing by rumor."

A consequence of this construct is that, even for the largest global networks, no single firm has a complete map of the Internet. The third function of function of the NOGs is sustaining the relationships within the routing community. *Maintaining* the integrity of the routing system requires substantive coordination and cooperation across network, firm, and international boundaries, often based on community relationships established and sustained at NOGs. Identifying, mitigating, and remediating operational failures and intentional shutdowns,[80] such as the Pakistan-YouTube incident, requires this cooperation. Networks regularly monitor their connectivity and can *identify* outages on their own. *Restoring* connectivity, though, requires coordination, often with multiple parties, to identify the source of the externality and who is necessary to restore normal operations.

Structured Operational Epistemic Authority: Regional Internet Registries (RIRs)

A key component of routing is distributing the information necessary to get traffic from one location to another, i.e. making sure everyone has the pieces of the map necessary to move data closer to its destination. For such a global network to function properly, for traffic to consistently get from an origin (such as a website) to a destination (a user's laptop browsing that website), the addresses of those origins, the intermediate stops along the way, and the final destination, must be globally unique. The primary function of the RIR system is to maintain accurate, up-to-date, globally accessible registries of the address information necessary for this consistency. Each

[77] Based on interviews and fieldwork, across the NOG community, sending marketing representatives is strongly discouraged by the community. They still show up, but if they cannot keep up with the technical vernacular and discussions, or prove to be disruptive, they are generally ignored, and on occasion, shunned.

[78] For detail on the contracting relationships see Clark, Lehr, and Bauer (2011) and Faratin et al. 2008.

[79] Faratin et al. 2008.

[80] See AccessNow's recent shutdown reports (Berhan 2020)taye2021shattered for analyses of recent shutdowns around the glob.

RIR maintains the authoritative information about which firms[81]have been delegated which addresses and network identifiers.[82] When Pakistan "hijacked" YouTube, it broke this global uniqueness rule,[83] violating resource policies established by the RIR system. Pakistan's (illegitimate, from the perspective of the RIR system) advertisement effectively claimed that it held the addresses that had been delegated to YouTube and corresponded to its services. Pakistan introduced conflicting information (a false rumor) into the routing system, (temporarily) creating an inconsistent map of the Internet.

The role of the RIR system is largely administrative, but critical to rule-making in the Internet. The RIRs also provide the fora in which the fundamental political questions of who gets what (addresses and network identifiers), and how, play out. They provide the fora in which the operational order (related to address resources) is discussed, negotiated, established, and maintained. The RIR system *coordinates* the bottom-up consensus processes for developing resource policy, the rules that determine how number resources are delegated, to whom, and under what conditions. The RIR (as a nonprofit firm) itself does not determine the substance of rules, but rather, it facilitates the consensus among operators in the address community that serve as both rule makers and rule takers, and maintains the authoritative records of these proceedings.

The five modern RIRs, listed in the order they were established, are:[84]

- Réseaux IP Européens Network Coordination Centre (RIPE NCC), established in 1992, located in The Netherlands, coordinating number resources for Europe, the Middle East, and Russia
- Asia-Pacific Network Coordination Centre (APNIC), established in 1993, located in Australia, coordinating number resources for the Asia Pacific region
- American Registry for Internet Numbers (ARIN), established in 1997, located in the United States, coordinating number resources for the United States, Canada, and some Caribbean and North Atlantic islands
- Latin American and Caribbean Internet Addresses Registry (LACNIC), established in 2002, located in Uruguay, coordinating number resources for Latin America and some Caribbean islands
- African Network Coordination Centre (AFRINIC), established in 2005, located in Mauritius, coordinating number resources for Africa

[81] Typically firms, but number resources have been delegated to individuals in the past. Most of these delegations are artifacts of the early, experimental Internet. Delegation to private individuals, especially during the period in which IPv4 addresses were becoming increasingly scarce, has been much less common in the modern Internet.

[82] These networks are numbers that uniquely identify a network as a whole. More technically, those identifiers, referred to as autonomous system numbers (ASNs) uniquely identify networks with a common routing policy, typically one per network (firm), but there are exceptions.

[83] More technically, it illegitimately appropriated resource rights exclusively delegated to YouTube by the RIR system.

[84] NRO 2021.

The RIRs coordinate through the Number Resource Organization (NRO), an organization jointly funded by the RIRs to help coordinate and support joint activities of the RIRs and to be an authoritative voice for the RIR system in broader Internet governance fora.[85]

In contrast to the diffuse structure and operational epistemic authority of the routing community and the NOGs, the criteria for establishing an Internet registry[86] and the constitutional norms of the RIRs[87] are formally (and authoritatively) established in IETF RFCs. The criteria for establishing a regional Internet registry highlight the foundations of bottom-up governance and endogenous legitimacy: networking authorities (i.e. experts, not necessarily government actors) in the region must legitimize the organization and that "the organization will commit appropriate resources to provide stable, timely, and reliable service to the geographic region."[88] The constitutional norms of the RIRs (below, from RFC2050) provide insight into the function of the RIR, its commitment to fair and responsible delegation of resources, and, most importantly, the commitment to bottom-up (rough) consensus processes.

Conservation: Fair distribution of globally unique Internet address space according to the operational needs of the end-users and Internet Service Providers operating networks using this address space. Prevention of stockpiling in order to maximize the lifetime of the Internet address space.

Routability: Distribution of globally unique Internet addresses in a hierarchical manner, permitting the routing scalability of the addresses. This scalability is necessary to ensure proper operation of Internet routing, although it must be stressed that routability is in no way guaranteed with the allocation or assignment of IPv4 addresses.

Registration: Provision of a public registry documenting address space allocation and assignment. This is necessary to ensure uniqueness and to provide information for Internet trouble shooting at all levels.[89]

In 2013, RFC7020 updated these constitutional norms to reflect modern number resources dynamics, in particular the impending depletion of the global pool of IPv4 addresses. Given the increasing scarcity of addresses, *conservation* was updated to *allocation pool management*, reaffirming that fairness means delegating resources to actors that can demonstrate operational need, not the highest bidder. *Routability* was updated to *hierarchical allocation* to limit unnecessary redundancy. *Registration* was updated to *registration accuracy*. The global pool of IPv4 addresses reached depletion on 3 February 2011, leaving only those remaining in regional pools for delegation. The means of acquiring IPv4 addresses began to shift from delegation from diminishing regional pools managed by the RIRs to transfers between firms.

[85] NRO 2020.
[86] Cerf 1990; Gerich 1993.
[87] Hubbard et al. 1996; Housley et al. 2013.
[88] Gerich 1993, 1-2.
[89] Hubbard et al. 1996.

Transfer policies have been some of the most contentious sets of policies developed in the RIR system. RIR policy requires transfers be mediated and approved by the RIR(s) that originally delegated those resources (and maintain registry data about those resources) to ensure registry accuracy necessary for network operations and the kinds of partial attribution necessary for security incident response.

The RIRs' constitutional norms were produced in the IETF RFC series as the authoritative documentation of standards, best practices, and procedures for the Internet. In keeping with the development of norms and procedures based on operational expertise, the authors of these documents are known experts on the RIR system, and were made authoritative through the IETF's consensus process. RFC2050 was the product of operational expertise early in the history of the modern Internet, laying the foundations of the RIR system. RFC7020 is an update of those constitutional norms to reflect new understandings of the dynamics of number resource management, especially in the face of IPv4 depletion, debates over precisely how transfers markets should function, and the increasing need for security protocols that could reinforce resource rights (reducing the potential for hijackings such as illustrated in the Pakistan-YouTube incident).

Both RFC2050 and RFC7020 highlight that:

> These goals may sometimes conflict with each other or with the interests of individual end users, Internet service providers, or other number resource consumers. *Careful analysis, judgment, and cooperation among registry system providers and consumers at all levels via community-developed policies are necessary to find appropriate compromises to facilitate Internet operations.*

Bottom-up consensus processes, derived from the IETF's rough consensus process, are the means by which the operational epistemic community develops resource delegation policy, evaluates the trade-offs when these norms conflict, and adapts policy to address those trade-offs and the needs of modern operational issues related to the delegation and use of numbers.

Sustaining Authority via Rough Consensus

Rough consensus not only serves to shape the rules at play, but also serves as a means to sustain and update knowledge of how the systems works within and across the operational epistemic communities that manage the Internet. It is the mechanism by which participants, as "an" authorities, debate and establish resource policies as "the authoritative." Embedded in this process is a shared way of knowing, through shared operational experiences, and debates over the validity and implications of those experiences as applied to resource policy development. The rough consensus process itself, as a mechanism for constructive conflict, represents a shared notion of validity, especially in the active consensus process described below. Are assertions contributing to the development of a particular policy from "an" authority, and based on operational experience? Do assertions align with or update existing knowledge of Internet operations and functions?

There are three categories of actors involved in the RIRs resource policy development process. RIR staff coordinate and document the consensus process. Members of the routing community contribute to the evaluation of policy proposals and are the authors of proposals. Policy shepherds (members of the routing community that are also members of a given RIR), are experienced community members formally tasked with evaluating the appropriateness of the scope of policy proposals and providing guidance for authors through the policy. The following elaborates the model of the RIRs' "bottom-up" rough consensus process.[90]

Problem Identification

In the problem identification and evaluation phase, participants and policy shepherds determine

1. whether a problem exists and it is affecting a significant number of constituents (i.e., it is not particularistic to a group or technology) and
2. whether the problem is within the scope of the RIRs' remit.

These two criteria contribute to ensuring activities are part of the RIRs' common policy enterprise (resource policy) and do not fall outside the RIRs' sphere of authority. In the RIRs, problem identification occurs in a number of places: in "hallway conversations" where an individual feels out whether others in their professional network are experiencing similar issues; in general discussion on e-mail lists; and in formal presentations of current issues being faced in the day-to-day operation of the Internet. In each of these cases, an individual (or individuals) are sharing their experience with others, especially more experienced participants, to determine whether the issue warrants a proposal. It is common for an operator's presentation of their experience, originally intended to be informative, to be turned into a proposal to update resource policy.

The second part of problem identification is determining whether the problem is clearly stated and within the scope of the RIR's resource policy making remit. Formally, determining scope takes place shortly after a policy proposal is submitted. The proposal must present a problem relevant to address resource delegation (conservation, routability, and registration), the mechanics of registry function, or a correction to existing policy to improve clarity or remove ambiguities. The proposal must be tractable for the RIR to implement, without overstepping the bounds of the RIR's remit or authority. Prospective policy proposals are made publicly available, typically on the policy mailing list for that RIR. If the proposal is rejected, it is presented as such

[90] The RIRs' process was adapted from the IETF's rough consensus process. Some of the mechanics differ, but the implications for authority are the same. Of the variants of consensus processes observed in the broader set of operational epistemic authorities in the Internet's infrastructure, the RIRs process is most similar to that of the IETF.

with a justification. If it is accepted for evaluation by the community, it is announced as an active proposal and the process moves into the *active census* phase.

Active Consensus

In the active phase, participants debate the content of a given proposal until rough consensus is reached. Achieving active consensus means that participants have iteratively reviewed the proposal, considered valid proposed changes (either enhancements or contestations), and the discussion has reached a point where there are no further proposed changes. In terms of the content of the proposal, the solution must fit within the established objectives of the RIR. Efficacy and efficiency, in terms of the proposal's operational, technical, and economic implications, are the criteria by which proposals are evaluated. Debates consider the tractability and implications of the solution for RIR members (in their role as rule takers) and in terms of implementation by the RIR itself (in its role as rule implementer, monitor, and potential enforcer). During the active consensus phase, the RIR typically produces an impact analysis, providing evaluators with information about what would be necessary for the RIR to implement the proposal, such as changes to the registry, operational requirements, etc. as a means to understand the impact on the RIR as a firm. The impact analysis includes an evaluation of *(1)* the costs of implementing a given policy and *(2)* potential legal implications of the policy for the RIR.

Rough consensus, in both the IETF and the RIRs, does not mean that everyone has to agree. Rather, it means that all contestations have been addressed, a significant portion of those engaged in the discussion agree, and importantly, that the consensus process itself has been followed. Like the IETF, participants in RIRs' consensus processes eschew majoritarian voting as a form of credible knowledge assessment. Evaluating the merits and implications of a policy, takes place in in-person RIR meetings and/or on e-mail lists dedicated to policy evaluation.

Simply asserting "No, I do not agree," without a rationale for that contestation, is insufficient and will be ignored. Unqualified contestations, and those that are not grounded in the epistemic communities' shared way of knowing (operational experience, demonstrable effects) are not considered authoritative. To be considered valid and credible, contributions to the policy debate must either fit, or constructively update the epistemic community's authoritative image of the operational dynamics at hand. When debating substantive change, such as policies affecting resource rights transfers markets or resource rights security, the constructive conflict embedded in these dialogues often updates community knowledge based on real-world observations, evaluated for veracity and consistency by those participating.

In interviews, leadership and policy process shepherds were quick to highlight that a "shallow 51-49 victory" is not rough consensus. Under rough consensus, the *number* of actors supporting or contesting a given proposal *is not* the deciding factor. The credibility of the critique (vis-à-vis community knowledge) and the evaluation of the proposal are the deciding factors. For instance, minority participants have an equal voice that *must* be addressed by the group for the process to proceed. The group must reconcile the contestation by evaluating validity, credibility, and impact. If recognized as a valid contestation (i.e. others in the group support this, for instance by indicating they have also experienced the problem presented), the active consensus process continues to explore the solution space until that contestation is resolved to the satisfaction of the minority participant(s) *and* other expert ("an" authority) participants.

A fundamental premise of *rough* consensus is that *all* credible critiques must be reviewed, but *not all of them* will result in a change in the proposed policy. In the "easy" case, a critique may simply contest the wording to reduce ambiguity and improve clarity. In more substantive cases, the rationale and particular trade-offs characterizing a given solution are contested, and the group must iterate over alternate solutions. For instance, a common debate is improvement in the integrity (often related to security) of the system versus transaction costs of that solution. Discussions in the active phase evaluate the current solution, the current trade-offs and possible alternative trade-offs to identify other possible solutions that satisfy the overall objectives of the proposal. An important part of this process is that, at this point, the active participants in the process essentially become contributors, creating a sense of community contribution and ownership of this proposal. As such, the community of experts acting as "an" authorities are shaping proposals that may become policy, and consequently, authoritative.

The content of contestations may be incorporated into a proposal, may be iteratively refined to satisfy those presenting the contestation and the broader set of contributors, or may be discarded. In some valid contestations, the original solution is discarded, but iterative discussions identify an alternate solution that satisfies the premises of the critique is identified and incorporated into the proposal. In other cases, this process is followed, but the critique dismissed. To illustrate, returning the integrity-transaction costs trade-off, a minority of actors from smaller firms (networks) may argue that the for them, the relative transaction costs of a given proposal are much higher than for larger firms. This is a valid point: it is generally considered unfair to introduce policy that creates disproportionately high costs for some, but not all actors. That said, it is up to the community to decide how disproportionate it is and whether that prevails over the countervailing integrity concerns. If, for example, integrity is paramount and the community cannot identify an alternative that creates the same (or a similar) improvement in overall integrity, then the critique may be acknowledged (through discussion and evaluation), but ultimately dismissed (the proposal is not changed) on the grounds that overall integrity supersedes those transaction costs.

Another characteristic of rough consensus is that vote packing is not possible. Consider a simplified example adapted from Resnick (2014). Five participants are evaluating two proposals, one that is general purpose and less efficient, one that requires special hardware but is more efficient. Four of the five argue that general purpose is more valuable, while the fifth, that has easy access to the specialized hardware, argues for the fifth. The group has decided that general purpose solution is, overall, more desirable for a solution to be used by the broadest set of actors. Even if the fifth recruits ten, or even twenty more actors to support their argument, if no new information or arguments are brought to bear, then the rough consensus still holds. In rough consensus processes, the number of supporters is not the deciding factor. Rather, increasing the number of expert actors in the rough consensus process is intended to improve the chances of bringing *additional* credible information and knowledge to the process. The objective is to maximize the potential size of the solution trade-off space, adding credibility to the ultimate solution and ensuring that the best operational information and knowledge used in the process.

Taken together, reaching active consensus means that the evaluative dialogue has *(1)* explored the solution trade-off space by *(2)* systematically addressing credible contestations offered by active participants. Like consensus in the IETF[91], the integrity of the consensus process itself highly contingent on the actor(s) designated to determine that consensus has been reached. In the IETF, this is the working group chair(s); in the RIRs, this is the policy shepherd(s). In interviews, experienced shepherds have stressed that while there is no hard and set rule, a good rule of thumb is to ensure that approximately 70-80 percent of participants agree with the resulting solution. Equally important to the integrity of the process is that all of the participants feel that, even if their preferred solution(s) were not accepted, that the rough consensus process was followed.

Passive Consensus

Passive consensus is the opportunity for community members that did not follow every incremental change in the proposal to evaluate, and potentially offer a critique of, the proposal resulting from active consensus. Rough consensus, as the name implies, does not mean that everyone agrees, nor does it require participation by every member of the community. Many of the participants in rough consensus processes are volunteers—they are engineers and technicians for whom this is important to their day job, but not their primary activity. Over the life cycle of a policy proposal, there is typically of core set of engaged actors, but other contributors may come and go throughout the incremental and iterative active consensus process.

Under passive consensus, silence on a proposal is sufficient. The implication is that there are no new critiques of the current proposal. That said, critiques may arise. In some cases, such as the "easy" language clarification critique described earlier, changes can be made in the passive consensus phase. In others, a more substantive critique that introduces new information or knowledge that has not been addressed in the active phase, must be addressed. For these critiques, the proposal will return to the active consensus phase to be resolved. Once resolved, the proposal returns again to passive consensus. After this period, the proposal enters the final phase of rough consensus, process review.

[91] Resnick 2014.

Process Review

The last step of the rough consensus process is process review. Process review is typically conducted by either the board of the RIR and/or the policy shepherds as a collective to ensure the integrity of the consensus process itself. Process review does not further evaluate the content of the policy proposal itself. The process review is a double check on the legal implications of a policy and potential risks a particular policy may create for the RIR as the firm implementing and managing the registry itself. As such, process evaluators are playing the roles of legal and risk evaluators for the registry itself.

Implications for Global Governance

Modern societies increasingly depend on complex distributed technical systems. Understanding how order is created in these systems, and the sources of authority that shape that order, is essential for developing the policy and institutions necessary to effectively integrate these authorities into the broader global governance system. In the management of complex engineering systems, here in particular the Internet, understanding the loci of governance, the scope of those regimes' sphere of authority, the source of that authority, and how that authority is maintained is critical for understanding the implications for global governance. For policy analysis, distinguishing between governance *on* the Internet and governance *in* the Internet is a necessary first cut at mapping out the spheres of authority in this distributed, complex system. In this last section, the analytic implications are presented, with a brief foray into the normative implications for global governance. Governance on and governance in, and the concept of operational epistemic authorities, are presented in terms of their contributions to understanding Internet governance in the broader global governance system. Normatively, the good news is that these authorities have contributed to sustaining a valuable global communications system; the bad news is that the current ad hoc relationships with broader global governance institutions is unstable, especially in the face of contestations by illiberal regimes.

Governance in versus governance on is a simple, but important distinction that is often lost in broad characterizations of Internet governance as a form of private ordering, driven by private interests. Following the earlier distinction between multinationals managing platforms on the Internet and the operations communities presented here, these are both forms of private governance, but the kinds of issues they engage with, the scope of governance, and to whom they are accountable are significant. It also encourages the analyst to dig deeper into the diverse roles of actors within multinationals. Firms such as Google, Meta, and Amazon employ marketing teams and platform developers whose decisions shape the kinds of behaviors that play out on those platforms. These firms also employ network operators, security teams, and abuse desk operations teams that both distinguish themselves from the former (often adamantly), and express a normative dedication to the stability and security of the Internet. These actors balance their obligations to their job and the norms of OEAs; in a number of OEAs, it is a common norm to announce one's affiliation and in what capacity one is making a contribution or contestation.

The notion of OEAs contributes to the literature on private authority and ordering, the work on epistemic communities pioneered by Haas, and most specifically contributes to the typology of epistemic authorities offered by Zürn. The operational component means not just having access to resources, but includes the scope of authority and the norms shaping the willingness of an OEA to use their capabilities and capacities to sustain operational order. The operational component also speaks to the source of authority and how it accrued to these institutions. This distinguishes OEAs from Zürn's politically assigned epistemic authorities, which have been delegated authority, for whom political influence goes both ways (offering significant interpretations and having those interpretations influenced by exogenous factors), and for whom authority may be rescinded. Operational also distinguishes OEAs from Zürn's pure epistemic authorities, exemplified by human rights and civil society groups. Like pure epistemic authorities, whose authority is not politically assigned, OEAs derive their authority from a distinct (often transnational) polity. Unlike pure epistemic authorities, they are not trying to shape the order and governance of a system from the outside: OEAs directly manage the system, here in particular the routing and addressing systems of the Internet.

Incorporating Flathman's notions of "in" authority, "an" authority, and "the authoritative" provides a conceptual framework for understanding how authority is sustained, and, taken together with the norms and values of the community, how the scope of that authority remains the same, or changes. Following Flathman's overall characterization of authority,[92] these ideal forms are analytically useful, but are more powerful when the analyst evaluates how the mix of these two plays out to contribute to "the authoritative." It also highlights fundamental trade-offs. DOEAs minimize "in" authority relationships, in both the IETF and the routing community. Some routing norms and best practices are documented by the routing community, most notably in IETF RFCs and the Internet Society's MANRs project,[93] but there is no formal obligation to follow any of these practices short of those necessary for baseline functionality. They are authoritative in that it has been agreed they are a best practice, but they are not obligatory. In contrast, those receiving IP address delegations and transfers from the RIRs are contractually bound to adhere to resource policy. Resource policies are created by rough consensus, with checks to ensure the integrity of in the process validation phase, but compliance is monitored and enforced by a non-profit firm whose contracts confer a degree of "in" authority.

As implied by the comparison above, evaluating OEAs as a mix of "in" and "an" authority also provides a framework for evaluating epistemic quality and legitimacy.

[92] Flathman 1980.
[93] Internet Society 2022.

Zürn indicates that "an epistemic authority need not, in all cases, convince people factually and in detail. It is, therefore, not the quality of the specific argumentation, but rather the general reputation of an institution . . . that is decisive."[94] Characterization of the mix of "in" and "an" offers a means of evaluating the integrity of the process of creating and maintaining the authoritative, without necessarily "convinc[ing] people factually and in detail." The distinction here is not necessarily one of more or less "an" authority or "in" authority. Rather, it is a question of the integrity of the process of formulating the authoritative in terms of endogenous legitimacy and impartiality. Complementing evaluations of the institution's reputation, the OEA framework facilitates distinguishing institutions' authority structure in terms of opportunities for bias (lack of impartiality). Ongoing work is applying the OEA framework in a systematic comparative analysis of the broader set of OEAs engaged in managing Internet operations, including a novel comparative analysis of ICANN.

Normatively, the good news is that the epistemic authorities evaluated here are driven by a cooperative ethos, have demonstrated the capabilities and capacities to sustain the address and routing system, and regularly act to mitigate global externalities. Their focus on endogenous legitimacy is both a strength and a weakness. They have focused their scope of authority and intervention to operational issues, with exceptions limited to when the integrity of the system is impacted. Their aversion to intentionally interfering with public policy and broader transnational issues is laudable for their awareness of the limits of their knowledge and representativeness to make such decisions.

The bad news is that these institutions have largely informal relationships with the broader global governance system. Historically, these communities have avoided engagement with state actors. More recently, they have recognized the need to engage, in part recognizing the limitations of their own capabilities, capacities, and authority, and in part because policy entrepreneurs in both these communities and in governments and international organizations have recognized the need for engagement. While the relationships between these epistemic authorities and state-based authorities *do* exist, like these epistemic communities themselves, they are largely informal, and based on interpersonal relationships. In the case of the routing community, their diffuse structure limits engagement, although experts in these communities have engaged with regulatory bodies such as the United States' Federal Communications Commission (FCC) and the European Union's Body of European Regulators for Electronic Communications (BEREC) in their capacity as well known "an" authorities from industry. Not surprisingly, the RIRs have created more durable fora for engagement, developing working groups for educating and engaging with law enforcement, regulators, and policymakers.[95]

[94] Zürn (2018, 52), citing Haas (1992).

[95] For instance, ARIN has a longstanding history of working with and educating law enforcement. The RIPE NCC sustains an ongoing Round Tables forum for engaging with government representatives and regulators from its region on issues related to "the governance and operation of the Internet," (Réseaux IP

While these are valuable steps engaging with the broader global governance system, the informal character of these relationships makes these relationships tenuous. While there are certainly some actors in these communities that eschew government engagement, there are policy entrepreneurs among the leadership in these communities that recognize the need for engagement. Here, the these communities' self-imposed aversion to "making public policy" can be turned to diplomatic benefit. Many of these actors do want to provide credible advice to state and international actors wrestling with the distinctions between governance in and governance on, and the implications of policy for the liberal, innovative character of the Internet. Committing further analysis to how OEAs can effectively engage with state-based authorities, while continuing to ensure the integrity of their own image of authority, can substantively contribute to greater integration into the global governance system.

Supplementary Material

(This is dummy text) Supplementary material for this research note is available at <https://doi.org/10.1017/Sxxxxxxxxx>.

References

Abbate, Janet. 2000. *Inventing the Internet.* The MIT Press, July.

Abbate, Janet. 2017. What and Where Is the Internet? (Re)Defining Internet Histories. *Internet Histories* 1, nos. 1-2 (January):8–14. https://doi.org/10.1080/24701475.2017.1305836.

Becker, Manuel. 2019. When Public Principals Give up Control over Private Agents: The New Independence of ICANN in Internet Governance. *Regulation & Governance* 13 (4):561–576. https://doi.org/10.1111/rego.12250.

Bennett, Andrew, and Jeffrey T. Checkel, eds. 2015. *Process Tracing : From Metaphor to Analytic Tool.* Strategies for Social Inquiry. Cambridge University Press.

Berhan, Taye. 2020. Targeted, Cut Off, and Left in the Dark: The #KeepItOn Report on Internet Shudowns in 2019. Technical report. Https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf. Access Now.

Black, Julia. 2017. 'Says Who?' Liquid Authority and Interpretive Control in Transnational Regulatory Regimes. *International Theory* 9, no. 2 (April):286–310. https://doi.org/10.1017/S1752971916000294.

Blumenthal, M. S., and D. D. Clark. 2001. Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World. *ACM Transactions on Internet Technology (TOIT)* 1 (1):70–109.

Börzel, Tanja A., and Michael Zürn. 2021. Contestations of the Liberal International Order: From Liberal Multilateralism to Postnational Liberalism. *International Organization* 75 (2):282–305. https://doi.org/10.1017/S0020818320000570.

Européens Network Coordination Centre 2022).

Braman, Sandra. 2010. The Interpenetration of Technical and Legal Decision-Making for the Internet. *Information, Communication & Society* 13, no. 3 (April):309–324. https://doi.org/10.1080/13691180903473814.

Braman, Sandra. 2011. The Framing Years: Policy Fundamentals in the Internet Design Process, 1969–1979. *The Information Society* 27, no. 5 (October):295–310. https://doi.org/10.1080/01972243.2011.607027.

Braman, Sandra. 2013. The Geopolitical vs. the Network Political: Internet Designers and Governance. *International Journal of Media & Cultural Politics* 9, no. 3 (September):277–296. https://doi.org/10.1386/macp.9.3.277_1.

Büthe, Tim, and Walter Mattli. 2011. *The New Global Rulers: The Privatization of Regulation in the World Economy.* Princeton University Press.

Clark, David D. 1992. A Cloudy Crystal Ball: Visions of the Future. https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf. Plenary Presentation. Cambridge, MA, July.

Clark, David D., William Lehr, and Steven Bauer. 2011. Interconnection in the Internet: The Policy Challenge. SSRN Scholarly Paper ID 1992641. Https://papers.ssrn.com/abstract=1992641. Rochester, NY: Social Science Research Network, August.

Cutler, A. Claire, Virginia Haufler, and Tony Porter, eds. 1999. *Private Authority and International Affairs.* State University of New York Press.

David, Paul A. 2007. Path Dependence: A Foundational Concept for Historical Social Science. *Cliometrica* 1, no. 2 (April):91–114. https://doi.org/10.1007/s11698-006-0005-x.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance.* Information Revolution and Global Politics. The MIT Press.

Ellickson, Robert C. 1991. *Order without Law: How Neighbors Settle Disputes.* Harvard University Press.

Elmer-DeWitt, Philip, and David S. Jackson. 1993. First Nation in Cyberspace. *Time* 142, no. 24 (December):62.

Faratin, Peyman, David Clark, Steven Bauer, William Lehr, Patrick Gilmore, and Arthur Berger. 2008. The Growing Complexity of Internet Interconnection. Http://ezproxy.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eoh&AN=1095251&site=eds-live, *Communications and Strategies,* no. 72, 51–71.

Farrell, Henry, and Abraham L. Newman. 2021. The Janus Face of the Liberal International Information Order: When Global Institutions Are Self-Undermining. *International Organization* 75 (2):333–358. https://doi.org/10.1017/S0020818320000302.

Flathman, Richard E. 1980. *The Practice of Political Authority: Authority and the Authoritative.* Univ of Chicago Pr, August.

Frischmann, Brett M. 2012. *Infrastructure: The Social Value of Shared Resources.* Oxford University Press.

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences.* The MIT Press, February.

Greene, Barry. 2021. Network Operations Groups (NOGs). https://www.senki.org/network-operations-scaling/network-operations-groups-meeting/.

Haas, Peter M. 1992. Introduction: Epistemic Communities and International Policy Coordination. *International Organization* 46 (1):1–35. https://doi.org/10.1017/S0020818300001442.

Hafner, Katie, and Matthew Lyon. 1999. *Where Wizards Stay Up Late: The Origins Of The Internet.* Simon & Schuster, August.

Haigh, Thomas, Andrew L. Russell, and William H. Dutton. 2015. Histories of the Internet: Introducing a Special Issue of Information & Culture. *Information & Culture: A Journal of History* 50 (2):143–159. https://doi.org/10.1353/lac.2015.0006.

Hall, Rodney Bruce, and Thomas J. Biersteker, eds. 2003. *The Emergence of Private Authority in Global Governance.* Cambridge University Press, January.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2017. Between Coordination and Regulation: Finding the Governance in Internet Governance. *New Media & Society* 19, no. 9 (September):1406–1423. https://doi.org/10.1177/1461444816639975.

Internet Society. 2022. MANRS – Mutually Agreed Norms for Routing Security. https://www.manrs.org/.

Jongen, Hortense, and Jan Aart Scholte. 2021. Legitimacy in Multistakeholder Global Governance at ICANN. *Global Governance: A Review of Multilateralism and International Organizations* 27, no. 2 (June):298–324. https://doi.org/10.1163/19426720-02702004.

Klein, Hans. 2002. ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *Information Society* 18, no. 3 (May):193–207. https://doi.org/10.1080/01972240290074959.

Lake, David A. 2009. Relational Authority and Legitimacy in International Relations. *American Behavioral Scientist* 53, no. 3 (November):331–353. https://doi.org/10.1177/0002764209338796.

Lake, David A., Lisa L. Martin, and Thomas Risse. 2021. Challenges to the Liberal Order: Reflections on *International Organization*. *International Organization* 75 (2):225–257. https://doi.org/10.1017/S0020818320000636.

Layton, Edwin T. 1979. Scientific Technology, 1845-1900: The Hydraulic Turbine and the Origins of American Industrial Research. *Technology and Culture* 20, no. 1 (January):64–89. https://doi.org/10.2307/3103112.

Lijphart, Arend. 1999. *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries.* Yale University Press, July.

Mattli, Walter, and Tim Büthe. 2003. Setting International Standards: Technological Rationality or Primacy of Power? *World Politics* 56, no. 1 (October):1–42. https://doi.org/10.1353/wp.2004.0006.

Mattli, Walter, and Ngaire Woods. 2009. In Whose Benefit? Explaining Regulatory Change in Global Politics. In *The Politics of Global Regulation,* Kindle, 1–44. Princeton, NJ: Princeton University Press.

Moss, David A. 2004. *When All Else Fails: Government as the Ultimate Risk Manager.* Harvard University Press, October.

Mueller, Milton. 2002. *Ruling the Root.* The MIT Press.

NANOG. 2020. NANOG Bylaws. https://www.nanog.org/legal/bylaws/, July.

Noy, Chaim. 2008. Sampling Knowledge: The Hermeneutics of Snowball Sampling in Qualitative Research. *International Journal of Social Research Methodology* 11, no. 4 (October):327–344. https://doi.org/10.1080/13645570701401305.

NRO, The Number Resource Organization. 2020. About the NRO. https://www.nro.net/about/, November.

NRO, The Number Resource Organization. 2021. Regional Internet Registries. https://nro.net/about/rirs/, April.

Number Resource Organization. 2022. RIR Statistics | The Number Resource Organization. https://www.nro.net/about/rirs/statistics/.

Nye, Joseph S., and Robert O. Keohane. 1971. Transnational Relations and World Politics: An Introduction. *International Organization* 25 (3):329–349.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge University Press.

Raymond, Mark, and Laura DeNardis. 2015. Multistakeholderism: Anatomy of an Inchoate Global Institution. *International Theory* 7, no. 3 (November):572–616. https://doi.org/10.1017/S1752971915000081.

Réseaux IP Européens Network Coordination Centre. 2022. Roundtable Meetings. https://www.ripe.net/participate/meetings/roundtable/roundtable-meetings.

Cerf, V.G. 1990. IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status. RFC 1174. Fremont, CA, USA: IETF (Internet Engineering Task Force), August. https://doi.org/10.17487/RFC1174.

Gerich, E. 1993. Guidelines for Management of IP Address Space. Request for Comments, Internet Request for Comments 1466. Fremont, CA, USA: IETF (Internet Engineering Task Force), May. https://doi.org/10.17487/RFC1466.

Hubbard, K., M. Kosters, D. Conrad, D. Karrenberg, and J. Postel. 1996. Internet Registry IP Allocation Guidelines. Request for Comments 2050. Fremont, CA, USA: IETF (Internet Engineering Task Force), November. https://doi.org/10.17487/RFC2050.

Alvestrand, H. 2004. A Mission Statement for the IETF. Best Current Practice, Internet Request for Comments 3935. Fremont, CA, USA: Internet Engineering Task Force (IETF), October. https://doi.org/10.17487/RFC3935.

Rekhter (Ed.), Y., T. Li (Ed.), and S. Hares (Ed.) 2006. A Border Gateway Protocol 4 (BGP-4). RFC, Internet Request for Comments. Fremont, CA, USA: RFC Editor, January. https://doi.org/10.17487/RFC4271.

Housley, R., J. Curran, G. Huston, and D. Conrad. 2013. The Internet Numbers Registry System. RFC. Fremont, CA, USA: RFC Editor, August. https://doi.org/10.17487/RFC7020.

Resnick, P. 2014. On Consensus and Humming in the IETF. RFC 7282. Fremont, CA, USA: Internet Engineering Task Force (IETF), June. https://doi.org/10.17487/RFC7282.

Postel, J. 1981. Internet Protocol. RFC 791. Fremont, CA, USA: Internet Engineering Task Force (IETF), September. https://doi.org/10.17487/RFC0791.

RIPE NCC. 2008. YouTube and Pakistan Telecom. https://www.youtube.com/watch?v=IzLPKuAOe50, February.

Russell, A.L. 2006. 'Rough Consensus and Running Code' and the Internet-OSI Standards War. *IEEE Annals of the History of Computing* 28, no. 3 (July):48–61. https://doi.org/10.1109/MAHC.2006.42.

Sabel, Charles, Gary Herrigel, and Peer Hull Kristensen. 2018. Regulation under Uncertainty: The Coevolution of Industry and Regulation. Http://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12146, *Regulation & Governance* 12 (3):371–394.

Saltzer, J. H., D. P. Reed, and D. D. Clark. 1984. End-to-End Arguments in System Design. *ACM Transactions on Computer Systems* 2 (4):277–288.

Scott, Colin. 2015. The Contribution of Transnational Private Regulation to Revisiting Risk Regulation. Https://irgc.org/wp-content/uploads/2018/09/IRGC-IRR-2.pdf, *International Risk Governance Council,* Improving Risk Regulation:14.

Shoch, John F. 1978. Inter-Network Naming, Addressing, and Routing. In Proceedings of the Seventeenth IEEE Computer Society International Conference (COMPCON). Http://mailman.postel.org/ien/pdf/ien019.pdf. Washington D.C.: IEEE Computer Society, September.

Solum, Lawrence B. 2008. Models of Internet Governance. Technical report Law & Economics Research Paper No. LE08-027. University of Illinois Law.

Take, Ingo. 2012. Regulating the Internet Infrastructure: A Comparative Appraisal of the Legitimacy of ICANN, ITU, and the WSIS. *Regulation & Governance* 6, no. 4 (December):499–523. https://doi.org/10.1111/j.1748-5991.2012.01151.x.

TenHouten, Warren D. 2017. Site Sampling and Snowball Sampling - Methodology for Accessing Hard-to-Reach Populations. Http://www.jstor.org/stable/26411978, *BMS: Bulletin of Sociological Methodology / Bulletin de Méthodologie Sociologique,* no. 134, 58–61.

Underhill, Geoffrey R. D., and Xiaoke Zhang. 2008. Setting the Rules: Private Power, Political Underpinnings, and Legitimacy in Global Monetary and Financial Governance. Http : //www.jstor.org/stable/25144816, *International Affairs* 84 (3):535–554.

van Eeten, Michel JG, and Milton Mueller. 2013. Where Is the Governance in Internet Governance? *New Media & Society* 15, no. 5 (August):720–736. https://doi.org/10.1177/1461444812462850.

van Schewick, Barbara. 2010. *Internet Architecture and Innovation.* The MIT Press, July.

Yates, JoAnne, and Craig N. Murphy. 2019. *Engineering Rules: Global Standard Setting since 1880.* Johns Hopkins University Press, June.

Zittrain, Jonathan L. 2006. The Generative Internet. *Harvard Law Journal* 119:1974–2040.

Zürn, Michael. 2018. *A Theory of Global Governance: Authority, Legitimacy, and Contestation.* Oxford University Press. https://doi.org/10.1093/oso/9780198819974.001.0001.

Date received: MMMM DD, YYYY; Date accepted: MMMM DD, YYYY.

Dummy dates;
please ignore.

A Non-Technical Introduction to Cyber Policy
INTA 689

Fall 2020
Tuesdays 1330 - 1620
1041 Allen Building

Instructor: Jesse H. Sowell II
E-mail: jsowell@tamu.edu

Office: 1096 Allen Building
Office Hours: Tuesdays 1630–1800 by appointment

Course Description

The implications of cyber-enabled systems cross-cuts a diverse set of policy and public administration domains. This course provides non-technical students with a working understanding of cyber-enabled systems and their impact on policy and public administration tasks and processes. This introductory course will equip students with the skills and analytic frameworks necessary to effectively address the benefits and risks of cyber-enabled systems.

Course Prerequisites

There are no prerequisites for this course.

Special Course Designation

This course is what Texas A&M and the Bush School refer to as a "W" course for "writing intensive." In addition to the substance of the course, this course will also help you hone your critical thinking skills and the skills necessary to write effective, objective, evidence-based policy analyses and memos. These skills will be stressed in the evaluation of your policy research project.

Course Learning Outcomes

The learning objectives described below represent concepts and ways of thinking you come away from after this course. They also represent the what you will be evaluated on overall as the course proceeds. You are expected to have an understanding of the high-level concepts outlined below, using your policy research project to begin developing your expertise in a particular domain (or set of domains!) of cyber policy and cybersecurity. Below, these concepts are highlighted in terms of the *substantive* concepts you are expected to master, and how you will be *evaluated* (such as in class discussions, presentations, or written assignments such as the midterm and your policy research project). *Specific learning objectives for each assignment can be found in the Assignments section of this syllabus.*

Cyber Policy and Cybersecurity

Each of these learning objectives will be evaluated in terms of

1. how accurately you articulate the key concepts and issues at play, highlighting the current debates and
2. how effectively and appropriately you use these concepts in discussions, class presentations, the midterm, and your policy research project.

The substantive learning objectives for this course are to:

- understand and critically evaluate the role of transnationalism in the context of cyber policy and cybersecurity in class discussions and written assignments
- evaluate the changing capabilities and capacities of state and non-state actors relative to managing the Internet's infrastructure, and their implications for cyber policy and cybersecurity in class discussions and your policy research project
- evaluate the current debate on Internet "consolidation" using both the Internet Society's notion of Internet invariants and Zittrain's notion of generativity
- have a familiarity with the rough mechanics of the Internet's infrastructure and how it functions as a "network of (largely) private networks" and be able to use this analytically in class discussions and written assignment, in particular in the midterm
- describe the diverse institutional landscape that makes up the cyber regime complext, distinguishing between cyber norms, the cyber regime complex, and evaluating the implications for coalition building, in particular applying these concepts in your policy research project
- define the attribution problem and the challenges of the "Internet jurisdiction" problem as a fundamental challenge to international cyber policy and cybersecurity, evaluated in particular in your midterm essay on this topic
- describe and evaluate the early and modern network neutrality debate, from the context of how traffic moves across the Internet, and notions of access (the digital divide) and innovation, evaluated in terms of class discussion and a midterm essay question, and as appropriate for policy research projects
- understand the fundamentals of encryption, then contrast the arguments in the recent "going dark" debate, in particular their implications for national security, surveillance, and freedom of speech in class discussion, a midterm question, and as appropriate in policy research projects
- describe the role and challenges of Internet infrastructure development in terms of its contribution to public, private, and social goods in class discussion and as appropriate for policy research projects
- understand and evaluate the implications of Internet communication for privacy, the potential for censorship, and human rights in class discussions and written assignments
- distinguish between various forms of fake news and disinformation, in particular from the perspective of the incentives of actors to engage in disinformation and the capabilities and capacities of both state and non-state actors in class discussions and as appropriate to your policy research project
- describe the basic political economy of cybersecurity and the collaborative challenges to mitigating and remediating transnational cybercrime in class discussions and as appropriate to policy research projects
- evaluate international efforts to develop norms around cyberwarfare, the debates around developing effective statecraft, and how the notions of deterrence and coercion differ in the context of cyber operations in class discussions and as appropriate for policy research projects

Writing

The focus of the writing learning objectives is to develop systematic strategies for critically evaluating a policy issue, then conveying a balanced analysis and recommendations. These learning objectives will be stressed in each of the course assignments. The overall learning objectives for the writing portion of this course are to:

- succinctly *summarize* a cyber policy or security issue for a policy or intelligence audience
- critically evaluate credible options in an unbiased way, presenting the audience with a balanced view of the issues, potential solutions, and implications
- narrow a broad issue (such as encryption) to a tractable issue salient to policy makers or the intelligence community
- effectively use evidence from the literature, government and industry reports, and the media to effectively support articulations of solutions and recommendations
- effectively use detailed outlines to identify which background concepts contribute to the narrower argument and how these will be used as the connective logic in analyses and recommendations
- effectively use detailed outlines to develop the articulation of an argument, in particular to evaluate the flow of the argument and differentiate what literature and cases are essential to the overall argument
- use the proposal, detailed outline, and final draft to recognize that the argument and structure will

evolve over multiple iterations and refinements

Textbooks and Resource Materials

Books

There are no textbooks assigned for this course. All of the course materials can be found in the shared Zotero library, described below.

IR Background Readings

While this course focuses on cyber policy, in particular from a neoliberal institutionalist perspective, the course will draw on some of the core concepts in international relations. The following provides some core readings that international affairs students are expected to be familiar with. You do not have to go read each word-for-word, but you should be familiar with the key ideas.

Finnemore, Martha and Kathryn Sikkink (1998). “International Norm Dynamics and Political Change’’. In: *International Organization* 52.4. http://www.jstor.org/stable/2601361, pp. 887–917.

Gourevitch, Peter (1978). “The Second Image Reversed: The International Sources of Domestic Politics’’. In: *International Organization* 32.4, pp. 881–912. DOI: 10.1017/S002081830003201X.

Haas, Peter M. (1992). “Introduction: Epistemic Communities and International Policy Coordination’’. In: *International Organization* 46.1, pp. 1–35. DOI: 10.1017/S0020818300001442.

Keohane, Robert O. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton, New Jersey: Princeton University Press.

——— (2011). “Global Governance and Legitimacy’’. In: *Review of International Political Economy* 18.1, pp. 99–109.

Keohane, Robert and Jr Joseph S. Nye (2001). “Between Centralization and Fragmentation: The Club Model of Multilateral Cooperation and Problems of Democratic Legitimacy’’. In: *SSRN eLibrary.*

Koremenos, Barbara, Charles Lipson, and Duncan Snidal (2001). “The Rational Design of International Institutions’’. In: *International Organization* 55.4. http://www.jstor.org/stable/3078615, pp. 761–799.

Krasner, Stephen D. (1982). “Structural Causes and Regime Consequences: Regimes as Intervening Variables’’. In: *International Organization* 36.2. http://www.jstor.org/stable/2706520, pp. 185–205.

——— (1983). *International Regimes.* 1st edition. Ithaca, NY: Cornell University Press.

Lake, David A., Lisa L. Martin, and Thomas Risse (2021). “Challenges to the Liberal Order: Reflections on *International Organization*’’. In: *International Organization* 75.2, pp. 225–257. DOI: 10.1017/S0020818320000636.

March, James G. and Johan P. Olsen (1998). “The Institutional Dynamics of International Political Orders’’. In: *International Organization* 52.4. http://www.jstor.org/stable/2601363, pp. 943–969.

Nye, Joseph S. and Robert O. Keohane (1971). “Transnational Relations and World Politics: An Introduction.’’ In: *International Organization* 25.3, pp. 329–349.

Ruggie, J.G. (1993). “Territoriality and beyond: Problematizing Modernity in International Relations’’. In: *International Organization* 47.1, pp. 139–174.

Ruggie, John Gerard (1992). “Multilateralism: The Anatomy of an Institution’’. In: *International Organization* 46.3. http://www.jstor.org/stable/2706989, pp. 561–598.

Waltz, Kenneth N. (2001). *Man, the State, and War: A Theoretical Analysis.* Second. https://www.jstor.org/stable/10.7312/walt12537. Columbia University Press.

Course Tools

The following provides an introduction to Zotero and Turnitin, our two primary course tools.

Zotero

We will be using Zotero to access course materials and to manage the references used in their course assignments. Students can find any of the materials listed on this syllabus in the shared Zotero library for this course. These materials include journal articles, conference papers, newspaper and magazine articles, **lecture slides**, and **the most up-to-date version of this syllabus**. Dr. Sowell will be sending invitations to the Zotero shared library after the first lecture, the afternoon of Tuesday 31 August 2021. If the student has not received an invitation to the shared library, check your spam folder. If the student still cannot find the invitation, e-mail Dr. Sowell (jsowell@tamu.edu).

The first step to using Zotero is to create a Zotero account. Students can download the Zotero app at https://www.zotero.org/download/. Students should also install the Zotero Connector for the browser of their choice. For step-by-step instructions, see the section on Zotero Configuration in the Appendix. Word processor plugins are available for Word, LibreOffice, and Google Docs.

TAMU libraries offers extensive documentation and tutorials on using Zotero. Please see:

- TAMU Zotero Research Guide
- Creating Bibliographies, in particular, the *two-minute* video that shows how to insert in-text citations into a Word document and how to generate bibliographies.
- The *less than two-minute* quick guide video for saving citations from your web browser

It should take less than 30 minutes to get the Zotero app and connector installed, setup, and then run through the two video guides. This will save you many more hours fiddling with references when writing your policy research projects.

Lecture slides will be added to the shared library at latest one hour before each class. The syllabus and class readings will be periodically updated with contemporary readings from the news related to upcoming topics in the course. To ensure you have the latest syllabus, it is strongly suggested that you open the syllabus directly from Zotero.

To be clear on the locations of these materials:

- the latest syllabus can always be found in the directory `INTA 689 - Cyber Policy/Syllabus` (Zotero calls directories *collections*) of the shared library
- slides will be in the collection `INTA 689 - Cyber Policy/Classes/ClassXX/Slides` where `XX` is the class number (01, 08, 12, etc.)
- references in slides that are not from one of the assigned books or one of the readings lists, can also be found in the `Slides` collection for that lecture

Two immediate points on using Zotero:

1. ***Become familiar with and use the Zotero app.*** You really only need the web interface to setup your account, setup your project library, and invite Dr. Sowell to your project library. After that, the bulk of your work will be ***in the Zotero app.***
2. ***Make sure to regularly refresh your Zotero libraries*** using the little green arrow in the upper right of the Zotero app. This ensures that all of *your* material is sync'd so Dr. Sowell can see it and help you where necessary, and it makes sure you have the latest course materials, including the latest version of this delightful document (the syllabus).

Please contact Dr. Sowell (jsowell@tamu.edu) if you have any problems accessing Zotero or the class materials in the shared library `INTA 689 - Cyber Policy`.

Project Deliverables via Turnitin

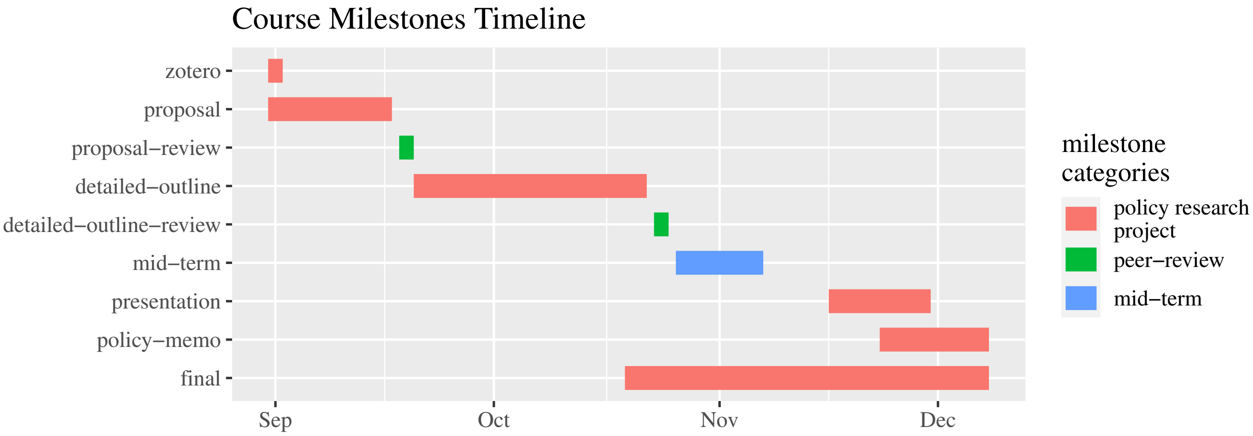
Policy research project milestones, the midterm, and presentation deliverables will be turned in via Turnitin. These will be due **at or before 2359 on the assignment due date**. Dr. Sowell will send invites to students' `@tamu.edu` e-mail addresses after the first lecture. Specific instructions for assignment deliverables are described along with the corresponding assignment.

Grading and Overview of Assignments

Details and guidelines for each assignment are provided in Assignments. Assignments contribute to your final grade as follows:

1. participation, 10%, *4* points of which is writing a peer review
2. one presentations of class readings by students, 10%
3. one policy memo on policy research project, 10%, due **Wednesday 08 December 2021** along with final draft of policy research project
4. take-home mid-term, 20%, distributed **Tuesday 26 October 2021** and due **at or before 2359 on Sunday 07 November 2021**.
5. policy research project (total 50%) and peer reviews (total 4% of participation), breakdown:
   - setup shared policy research project library in Zotero, 3 participation points, due Thursday 02 September 2021
   - proposal, 10%, due Friday 17 September 2021
   - proposal peer review, 2%, due Monday 20 September 2021
   - detailed outline, 15%, due Friday 22 October 2021
   - detailed outline peer review, 2%, due Monday 25 October 2021
   - in class presentation, 5%, due Tuesday 30 November 2021
   - final project report, 20%, due Wednesday 08 December 2021

Grades for assignments will be in terms of total points for the class. For instance, a perfect grade for a presentation of class readings would be 10/10.



After the midterm and a couple of weeks before the final you will get a grade report summarizing your grades and the class grade distribution.

Final letter grades will be assigned as follows:

letter grade	range
A	> 90%
B	>= 80%, < 90%
C	>= 70%, < 80%
F	< 70%

In terms of evaluation, grades for written assignments (within the scope of the assignment) are assessed as follows:

- **A+, >= 96%** indicates
  - exceptional mastery of concepts at hand,
  - exceptional application of the concepts,
  - salient issues and concepts covered in the class are addressed,
  - appropriate trade-offs are discussed,
  - analysis is supplemented by contemporary instances of the problem from outside materials,
  - exceptional articulation, with an introduction to the problem, challenges, trade-offs, and recommendations where requested
- **A, >= 90%, <96%** indicates
  - accurate articulation of concepts at hand,
  - effective applicatin of the concepts,
  - *most* salient issues and concepts covered in the class are addressed,
  - appropriate trade-offs are discussed,
  - good articulation of the analysis with an introduction to the problem, challenges, trade-offs, and recommendations where requested
- **B, >= 80%, < 90%** indicates
  - accurate articulation of the concepts at hand,
  - effective application of the concepts,
  - only *some* key issues and concepts related the problem at hand are presented,
  - some trade-offs discussed in class are missing,
  - weak articulation of analysis, has only rudimentary introduction to the problem, challenges, trade-offs, and recommendations where requested
- **C, >= 70%, < 80%** indicates
  - inaccurate articulation of the concepts at hand,
  - weak or unclear application of the concepts,
  - significant key issues and concepts related to the problem at hand are missing or misconstrued,
  - limited discussion of trade-offs,
  - poor articulation of analysis, does not have a clear introduction to the problem, challenges, trade-offs, and recommendations where requested
- **F, < 70%** indicates
  - inaccurate representation of the concepts at hand,
  - little to no application of the concepts,
  - signifiant number of the key issues and concepts related to the problem at hand are missing or misconstrued,
  - very little discussion of trade-offs or single-sided,
  - writing is unclear and unstructured

Late Work Policy

Enforcement of the following late work policy is at the discretion of the instructor.

As noted in the discussion of Turnitin, *all assignments for this class are due at or before 2359 on the due date for the assignment.* **Late submissions will incur a penalty of 10% per day after the due date.** For instance, if the assignment is due on Monday and it is submitted via Turnitin on Wednesday, a 20% late penalty will be applied. *Assignments submitted on or after the tenth day after the deadline will receive zero points and will not be graded.*

Ideally, everyone plans ahead and gets work done ahead of time. That said, every student gets one *late submission mulligan.* Everyone gets behind at some point or finds they have several deliverables due at the same time and needs a little slack. If you see yourself heading for this situation, to use your mulligan you must e-mail the instructor *at least 24 hours before the deadline* to indicate you would like to take your mulligan, explain why, and when you think you can submit the work. The instructor will work with you to identify a reasonable revised deadline. You will likely get a day or two more time, a week is unacceptable with the exception of dire circumstances. *Like the overall late policy, the mulligan is also at the discretion of the instructor, so please do not abuse this generous option.*

Lectures and Readings

All journal articles, papers, newspaper articles, and other documents assigned in the reading lists below can be found in the shared Zotero library for this course. Lecture slides will be added to the appropriate Zotero shared folder at latest one hour before class.

For any given class there will be at most four readings lists:

- **Essential Readings** are the *required* readings from the textbooks and course materials.
- **Contemporary Readings** are *strongly recommended* after reading the essential readings.
- **Optional Readings** are *not required.* These readings may be referenced in lectures. Optional readings may also be useful starting points for policy research project research.
- **Technical References** are *not required.* These are the references Dr. Sowell draws on for describing and explaining particular elements of the Internet's function or issue areas.

Unless specific sections or page numbers are specified in text below the reference for the reading material, you are expected to read the entire document.

Class #01: Tuesday 31 August 2021

Overview of Cyber Policy

Cyber Policy covers a broad range of topics from infrastructure development, privacy, access rights, disinformation campaigns, and cyberwarfare. In this lecture we will survey the topics we will discuss in the course, highlighting the differences between policy issues that play out *on* the Internet versus policy issues *in* the Internet. We will conclude with a discussion of the distribution of capabilities and capacity amongst state and non-state actors: what combinations of these actors have the right tools to effectively manage cyber policy issues?

Part I: Foundations

Class #02: Tuesday 07 September 2021

The User Experience

The end user's Internet experience has evolved substantively since the inception of the Internet. In this lecture, we will take a brief look at this evolution in terms of the changes in capabilities—from static websites to complex online web applications to "app" based services on phones and tablets and on to the emerging market of Internet of Things devices. At each inflection point we will describe, explain, and evaluate how new threats have emerged, how effectively they have been countered, and emerging challenges (such as IoT botnets and crimeware as a service). The lecture will conclude by transitioning through the user's view of the architecture—the Internet has been lauded as an architecture of innovation, but will it (or has it already) evolved into an architecture of vulnerabilitiy and/or control?

Essential Readings

- **Nye, Joseph S. and Robert O. Keohane (1971). "Transnational Relations and World Politics: An Introduction.'' In: *International Organization* 25.3, pp. 329–349.**

  This is an IR classic, you will see shades of transnationalism in the discussion of the cyber regime complex and in discussions of non-state institutions throughout the course.

- **Internet Society (2019). *Internet Society Global Internet Report 2019: Consolidation in the Internet Economy.* https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf. Reston, VA: Internet Society.**

  Read Chapters 1–8.

  Pay close attention to the implications of consolidation for end users, such as the Facebook Basics program. Also note the distinct tone of stewardship of the Internet.

- **Zittrain, Jonathan L. (2006). "The Generative Internet'". In: *Harvard Law Journal* 119.**

  Read Sections I and II, pp. 1975–1996.

  The notion of generativity is considered on of the key factors contributing to the Internet as a economic and innovation engine. Make special note of the characteristics of 'ease of mastery' and 'accessibility'

- **Keohane, Robert O. and David G. Victor (2011). "The Regime Complex for Climate Change'". In: *Perspectives on Politics* 9.1. http://www.jstor.org/stable/41622723, pp. 7–23.**

  In reading this article, pay special attention to the characteristics of a regime complex, in particular the ideas around policy experiments by like-minded actors and epistemic quality. We will be coming back to these qualities, and the characteristics of a regime complex writ broadly, through the semester.

- **Nye, Joseph (2014). "The Regime Complex for Managing Global Cyber Activities'". In: *Global Commission on Internet Governance* PAPER SERIES: NO. 1. https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf.**

  Nye's regime complex illustrates the diversity of actors *interested* in the cyber policy endeavor. That said, as we will discuss at a high level here, and see through the remainder of the course, not all of these actors have the capabilities and capacity to actually influence the rules of the game, or the platforms and infrastructure that make up the web, online platforms, and/or the Internet.

- **Sowell, Jesse H. (2020). "Evaluating Competition in the Internet's Infrastructure: A View of GAFAM from the Internet Exchanges'". In: *Journal of Cyber Policy* 5.1, pp. 107–139. DOI: 10.1080/23738871.2020.1754443.**

  Along with the ISOC report above, this artilce illustrates the diversity of governance configurations across the function-specific institutions that manage platforms and infrastructures in the Internet. Here in particular we seemingly the same actors (large tech firms) participating in very different forms of governance. One question we will address in discussion is whether they are actually behaving differently and why.

Contemporary Readings

- **Couturier, Kelly (2015). "How Europe Is Going After Apple, Google and Other U.S. Tech Giants'". In: *The New York Times.* https://www.nytimes.com/interactive/2015/04/13/technology/how-europe-is-going-after-us-tech-giants.html.**

- **Smith, Noah "Big Tech Sets Up a 'Kill Zone' for Industry Upstarts'". In: *Bloomberg.com.* https://www.bloomberg.com/opinion/articles/2018-11-07/big-tech-sets-up-a-kill-zone-for-industry-upstarts.**

- **The Economist (2018). "American Tech Giants Are Making Life Tough for Startups'". In: *The Economist.* https://www.economist.com/business/2018/06/02/american-tech-giants-are-making-life-tough-for-startups.**

- **Swisher, Kara (2019). "Opinion | Taming the Apex Predators of Tech'". In: *The New York Times.* https://www.nytimes.com/2019/05/21/opinion/facebook-google-monopolies.html.**

- **Wheeler, Tom (2019). *Should Big Technology Companies Break up or Break Open?* https://www.brookings.edu/blog/techtank/2019/04/11/should-big-technology-companies-break-up-or-break-open/.**

Optional Readings

- **Daigle, Leslie (2019). *The Internet Invariants: The Properties Are Constant, Even as the Internet Is Changing.* https://www.thinkingcat.com/wordpress/2019-invariantsupdated/. Internet Society, p. 81.**

  This is a more nuanced articulation of the Internet invariants by one of the original architects of the work. Of particular interest is the historical context provided for each.

- **Khan, Lina M (2017). "Amazon's Antitrust Paradox''. In: *The Yale Law Journal* 126.3, pp. 710–805.**

- **Khan, Lina M. (2019). "The Separation of Platforms and Commerce''. In: *Columbia Law Review* 119.4. https://www.jstor.org/stable/26632275, pp. 973–1098.**

- **Zittrain, Jonathan L. (2008). *The Future of the Internet–And How to Stop It.* Yale University Press.**

  This is the book version of Zittrain's article above. Fun fact: Zittrain said if he wrote a sequel it would be entitled "Meh, We Tried"

Class #03: Tuesday 14 September 2021

Mapping the Internet

Picking up with our discussion of the implications of the architecture for the end user, we will peel back the application layer and explore the underlying network that delivers the end user's experience. The *Inter*net is really a diverse network of (largely) private networks. We will visually explore how elements of this highly distributed infrastructure are interconnected, the notion of best effort service, how certain protocols serve as the "glue" that ensure effective coordination amongst networks based in many different economies. We will conclude by highlighting the fundamentally transnational character of the communication infrastructure, dispelling the conventional International relations argument that technical issues are simple coordination problems.

Essential Readings

- **Internet Society (2019). *Internet Society Global Internet Report 2019: Consolidation in the Internet Economy.* https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf. Reston, VA: Internet Society.**

  Revisit the discussions of the Internet's infrastructure.

Contemporary Readings

- **Dorman, Bob (2016). *How the Internet Works: Submarine Fiber, Brains in Jars, and Coaxial Cables.* https://arstechnica.com/information-technology/2016/05/how-the-internet-works-submarine-cables-data-centres-last-mile/.**

- **Satariano, Adam, Karl Russell, Troy Griggs, Blacki Migliozzi, and Chang W. Lee (2019). "How the Internet Travels Across Oceans''. In: *The New York Times*. https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html.**

Technical Readings

- **Faratin, Peyman, David Clark, Steven Bauer, William Lehr, Patrick Gilmore, and Arthur Berger (2008). "The Growing Complexity of Internet Interconnection''. In: *Communications and Strategies.* http://ezproxy.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eoh&AN=1095251&site=eds-live, pp. 51–71.**
- **Clark, David D., William Lehr, and Steven Bauer (2011). *Interconnection in the Internet: The Policy Challenge.* SSRN Scholarly Paper ID 1992641. https://papers.ssrn.com/abstract=1992641. Rochester, NY: Social Science Research Network.**

Class #04: Tuesday 21 September 2021

The Institutional Landscape

Now that we have a working map of the Internet, we will turn to mapping the constellation of transnational, non-state institutions that ensure the Internet remains connected in a secure and stable way. Since the NSF divested itself of its role managing the Internet's infrastructure, the engineers and operators now managing the infrastructure had to find governance solutions for managing a decentralized, transnational infrastructure. We will describe, explain, and evaluate the decentralized constellation of transnational, yet function-specific institutions that manage critical Internet resources. Thus far, the interests of these institutions have aligned with the public interest, but, to ensure this continues, we need to improve the lines of communications between these institutions and state actors.

Essential Readings

- **Choucri, Nazli and David D. Clark (2013). "Who Controls Cyberspace?'' In: *Bulletin of the Atomic Scientists* 69.5, pp. 21–31. DOI: 10.1177/0096340213501370.**
- **Eeten, Michel JG van and Milton Mueller (2013). "Where Is the Governance in Internet Governance?'' In: *New Media & Society* 15.5, pp. 720–736. DOI: 10.1177/1461444812462850.**
- **Henriksen, Anders (2019). "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace''. In: *Journal of Cybersecurity* 5.1. DOI: 10.1093/cybsec/tyy009.**

Contemporary Readings

- **Bund, Jakob and Patryk Pawlak (2017). "Minilateralism and Norms in Cyberspace''. In: *European Union Institute for Security Studies.***
- **Sukumar, Arun M. (2017). *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?* https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.**
- **Maurer, Tim and Kathryn Taylor (2018). *Outlook on International Cyber Norms: Three Avenues for Future Progress.* https://carnegieendowment.org/2018/03/02/outlook-on-international-cyber-norms-three-avenues-for-future-progress-pub-75704.**

Optional Readings

- **Finnemore, Martha and Duncan B. Hollis (2016). "Constructing Norms for Global Cybersecurity''. In: *American Journal of International Law* 110.3, pp. 425–479. DOI: 10.1017/S0002930000016894.**
- **Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis (2013). "Internet Security and Networked Governance in International Relations''. In: *International Studies Review* 15.1, p. 86. DOI: 10.1111/misr.12024.**

- Mueller, Milton L. (2010). *Networks and States: The Global Politics of Internet Governance.* The MIT Press.
- Mueller, Milton (2002). *Ruling the Root.* Cambridge, MA: The MIT Press.
- Goldsmith, Jack and Tim Wu (2008). *Who Controls the Internet?: Illusions of a Borderless World.* 1s edition. New York: Oxford University Press.
- Tikk, Eneken and Mika Kerttunen (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy.* Cyber Policy Institute.
- Diplomat The, Elaine Korzak (2017). *UN GGE on Cybersecurity: The End of an Era?* https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.
- Soesanto, Stefan and Fosca D'Incau (2017). *The UN GGE Is Dead: Time to Fall Forward.* https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.
- Grigsby, Alex (2017). *The Year in Review: The Death of the UN GGE Process?* https://www.cfr.org/blog/year-review-death-un-gge-process.

Class #05: Tuesday 28 September 2021

Attribution and "Internet Jurisdiction"

Attribution and jurisdiction problems confound a number of transnational issues that play out in and on the Internet. In a decentralized Internet, assigning attribution for a given set of actions (such as whether a particular individual viewed a given webpage at a certain time, or who is responsible for the latest DDoS attack) is very difficult (some have argued impossible). The global, yet decentralized character of the Internet also creates jurisdiction conflicts. For instance, online services produced in one jurisdiction may be illegal in others. In other cases, such as online attacks that rely on (illicitly appropriated) resources distributed across many jurisdictions, create substantive coordination and collaboration problems amongst both private cybersecurity actors and law enforcement. In this lecture, we will review a number of the seminal cases that highlight the challenges of attribution and jurisdiction conflicts, describing which aspects of these these problems have working solutions and which remain challenging.

Essential Readings

- Johnson, David R. and David G. Post (1996). "Law and Borders - the Rise of Law in Cyberspace’’. In: *Stanford Law Review* 48. https://papers.ssrn.com/abstract=535.
- Reidenberg, Joel R. (2005). "Technology and Internet Jurisdiction’’. In: *University of Pennsylvania Law Review* 153.6, pp. 1951–1974. DOI: 10.2307/4150653.
- Clark, David D. and Susan Landau (2011). "Untangling Attribution’’. In: *Harvard National Security Journal.* https://heinonline.org/HOL/P?h=hein.journals/harvardnsj2&i=531, pp. 323–352.
- Lin, Herbert (2016). "Attribution of Malicious Cyber Incidents: From Soup to Nuts’’. In: *Journal of International Affairs* 70.1. https://www.jstor.org/stable/90012598, pp. 75–137.

Optional Readings

- Zittrain, Jonathan (2005). *Jurisdiction.* 1st edition. Internet Law Series. New York: Foundation Press.
- Kohl, Uta (2007). *Jurisdiction and the Internet.* Cambridge University Press.

Class #06: Tuesday 05 October 2021

Network Neutrality

Network neutrality is one of the oldest debates in Internet policy. Oversimplifying, the argument is that all traffic on the Internet should be treated equally. In this lecture we will dig into the nuance of the network neutrality debate, highlighting the economic perspective as well as those that incorporate notions of fairness, innovation, and censorship. We will not only look at how the debate has evolved in the US, but also in other economies, such as Singapore, the Netherlands, and elsewhere (also linking this back to some of our core Internet jurisdiction conflicts). As with many things, this debate is fundamentally about economics—we will conclude our discussion by foreshadowing how issues of infrastructure development (in the next lecture) affect network neutrality.

Essential Readings

- **Stover, Christine M. (2010). "Network Neutrality: A Thematic Analysis of Policy Perspectives Across the Globe''. In: *Global Media Journal, Canadian ed.; Ottawa* 3.1. https://search.proquest.com/docview/888154405/abstract/7C4DD02817A84F03PQ/1, p. n/a.**
- **Wu, Tim (2003). "Network Neutrality, Broadband Discrimination''. In: *Journal on Telecommunications & High Technology Law* 2. https://heinonline.org/HOL/P?h=hein.journals/jtelhtel2&i=145, pp. 141–176.**
- **Yoo, Christopher S. (2005). "Beyond Network Neutrality''. In: *Harvard Journal of Law & Technology*. https://heinonline.org/HOL/P?h=hein.journals/hjlt19&i=4, pp. 1–78.**

Contemporary Readings

- **Ruiz, Rebecca R. (2015). "F.C.C. Sets Net Neutrality Rules''. In: *The New York Times*. https://www.nytimes.com/2015/03/13/technology/fcc-releases-net-neutrality-rules.html.**
- **Ruiz, Rebecca R. and Steve Lohr (2015). "F.C.C. Approves Net Neutrality Rules, Classifying Broadband Internet Service as a Utility''. In: *The New York Times*. https://www.nytimes.com/2015/02/27/technology/net-neutrality-fcc-vote-internet-utility.html.**
- **Collins, Keith (2018). "Net Neutrality Has Officially Been Repealed. Here's How That Could Affect You.'' In: *The New York Times*. https://www.nytimes.com/2018/06/11/technology/net-neutrality-repeal.html.**
- **Lapowsky, Issie (2017). "It's Super Hard to Find Humans in the FCC's Net Neutrality Comments''. In: *Wired*. https://www.wired.com/story/bots-form-letters-humans-fcc-net-neutrality-comments/.**
- **Pruitt, Courtney and Chris Roat (2017). *Bot or Not?: Verifying Public Comments on Net-Neutrality*. https://medium.com/ragtag-notes/bot-or-not-verifying-public-comments-on-net-neutrality-8c77ee54a02e.**
- **Kang, Cecilia (2019). "Net Neutrality Repeal at Stake as Key Court Case Starts''. In: *The New York Times*. https://www.nytimes.com/2019/02/01/technology/net-neutrality-repeal-case.html.**
- **Condliffe, Jamie (2019). "The Week in Tech: We Might Be Regulating the Web Too Fast''. In: *The New York Times*. https://www.nytimes.com/2019/04/12/technology/tech-regulation-too-fast.html.**

Optional Readings

- **Yoo, Christopher S. (2008). "Network Neutrality, Consumers, and Innovation Law in a Networked World''. In: *University of Chicago Legal Forum*. https://heinonline.org/HOL/P?h=hein.journals/uchclf2008&i=181, pp. 179–262.**

- **Wallsten, Scott and Stephanie Hausladen (2009). "Net Neutrality, Unbundling, and Their Effects on International Investment in Next-Generation Networks' ". In: *Review of Network Economics* 8.1. DOI: 10.2202/1446-9022.1171.**
- **Frischmann, Brett M. (2012). *Infrastructure: The Social Value of Shared Resources.* New York, NY, USA: Oxford University Press.**
- **Marsden, Christopher T. (2017). *Network Neutrality: From Policy to Law to Regulation.* Manchester University Press. DOI: 10.26530/OAPEN_622853.**

Class #07: Tuesday 12 October 2021

Reading Week

We will not have class this week. You should use this time to work on your detailed outlines.

Class #08: Tuesday 19 October 2021

Encryption and "Going Dark"

Encryption is the technical response to privacy and surveillance. In simple terms, encryption is the process of obscuring the content of a message. While a seemingly simple process, it has given rise to one of the oldest and most heated debates related to Internet technology. In this lecture, we will review how this debate evolved and its role in the contemporary "going dark" debate. In the first part of this lecture we will provide a high level, nontechnical overview of encryption and cryptography. We will then review the US and other states' attempts at regulating encryption. We will then dive into the "going dark" debate, the arguments that strong encryption, that cannot be broken by state actors, are limiting the abilities of legitimate law enforcement and intelligence agencies to perform investigations. Finally, we will revisit the regulatory discussion, how states are attempting to avoid "going dark," from requiring access to encryption keys, limiting the strength of commercially available encryption, and requiring "backdoors" into commercial security tools. To illustrate, we will review a few cases, in particular the recent standoff between Apple and the US Government.

Essential Readings

- **Swire, Peter P. and Kenesa Ahmad (2012). "Encryption and Globalization' ". In: *The Columbia Science & Technology Law Review* 13.Spring. DOI: 10.2139/ssrn.1960602.**
- **Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner (2015). "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications' ". In: *Journal of Cybersecurity* 1.1, pp. 69–79. DOI: 10.1093/cybsec/tyv009.**
- **Swire, Peter (2012). "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud' ". In: *International Data Privacy Law* 2.4, pp. 200–206. DOI: 10.1093/idpl/ips025.**
- **Swire, Peter and Kenesa Ahmad (2011). *'Going Dark' Versus a 'Golden Age for Surveillance'.* https://fpf.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf.**
- **Gasser, Urs, Nancy Gertner, Jack L. Goldsmith, Susan Landau, Joseph S. Nye, David O'Brien, Matthew G. Olsen, Daphna Renan, Julian Sanchez, Bruce Schneider, Larry Schwartzol, and Jonathan L. Zittrain (2016). *Don't Panic: Making Progress on the "Going Dark" Debate.* https://dash.harvard.edu/handle/1/28552576.**

- **Pfefferkorn, Riana (2017).** ***The "Going Dark" Debate: No News Isn't Necessarily Good News.*** **http://cyberlaw.stanford.edu/blog/2017/07/going-dark-debate-no-news-isn%E2%80%99t-necessarily-good-news.}**

Contemporary Readings

- **Kahn, Matthew (2017).** ***Deputy Attorney General Rod Rosenstein Remarks on Encryption.*** **https://www.lawfareblog.com/deputy-attorney-general-rod-rosenstein-remarks-encryption.**
- **Tait, Matt (2017).** ***Decrypting the Going Dark Debate.*** **https://www.lawfareblog.com/decrypting-going-dark-debate.**
- **Lichtblau, Eric and Katie Benner (2016). "F.B.I. Director Suggests Bill for iPhone Hacking Topped \$1.3 Million' '. In:** ***The New York Times.*** **https://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html.**
- **Lichtblau, Eric and Katie Benner (2016). "Apple Fights Order to Unlock San Bernardino Gunman's iPhone' '. In:** ***The New York Times.*** **https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.**
- **Manjoo, Farhad (2016). "Apple's Stance Highlights a More Confrontational Tech Industry' '. In:** ***The New York Times.*** **https://www.nytimes.com/2016/02/18/technology/apples-stance-highlights-a-more-confrontational-tech-industry.html.**
- **Shear, Michael D., David E. Sanger, and Katie Benner (2016). "In the Apple Case, a Debate Over Data Hits Home' '. In:** ***The New York Times.*** **https://www.nytimes.com/2016/03/14/technology/in-the-apple-case-a-debate-over-data-hits-home.html.**
- **Markoff, John, Katie Benner, and Brian X. Chen (2016). "Apple Encryption Engineers, If Ordered to Unlock iPhone, Might Resist' '. In:** ***The New York Times.*** **https://www.nytimes.com/2016/03/18/technology/apple-encryption-engineers-if-ordered-to-unlock-iphone-might-resist.html.**

Part II: Contemporary Issues

Class #09: Tuesday 26 October 2021

Infrastructure Development

In this lecture we dig a little deeper into the economics of Internet infrastructure development, focusing on the power dynamics between large incumbent networks and medium to small networks. In particular, we will further develop the role of the submarine cable networks and Internet exchanges. We will evaluate infrastructure development from three perspectives: the relative costs of each of thes different parts of the infrastructure; the roles they play in local and regional economies; and the vulnerabiliites faced by these infrastructures. We will conclude by looking back at how development processes have shaped the debates we have discussed thus far and foreshadow the role of development in the lectures in the rest of Part II, stressing that, to understand many of these issues, it is necessary to understand how the underlying infrastructure developed and the power dynamics amongst those actors.

Essential Readings

- **Frischmann, Brett M. (2012).** ***Infrastructure: The Social Value of Shared Resources.*** **New York, NY, USA: Oxford University Press.**

  Skim the Introduction, paying attention to the infrastructure report card. Read Chapter 1 and 2. Skim Chapter 3 and 10. Then read Chapter 13. For those doing network neutrality and infrastructure development, you should read all of this at some point.

- **Sowell, Jesse H. (2013). "Framing the Value of Internet Exchange Participation''. In: *Proceedings of the 41st Research Conference on Communication, Information and Internet Policy.* Ed. by TPRC. Telecommunications Policy Research Consortium.**

  Read the Executive Summary, skim the paper, don't worry about the math.

- **Weller, Dennis and Bill Woodcock (2013). *Internet Traffic Exchange: Market Developing and Policy Challenges.* no. 207. https://www.oecd-ilibrary.org/science-and-technology/internet-traffic-exchange_5k918gpt130q-en. Paris: OECD.**

- **Kende, Michael and Charles Hurpy (2012). *Assessment of the Impact of Internet Exchange Points—Empirical Study of Kenya and Nigeria.* Report for the Internet Society 20945-144. Internet Society.**

Optional Readings

- **Sowell, Jesse H. (2013). "Framing the Value of Internet Exchange Participation''. In: *Proceedings of the 41st Research Conference on Communication, Information and Internet Policy.* Ed. by TPRC. Telecommunications Policy Research Consortium.**

Class #10: Tuesday 02 November 2021

Privacy, Censorship, and Human Rights

The decentralized character of the Internet creates substantive opportunities for surveillance. In this lecture we will present Nissenbaum's notion of privacy as contextual integrity as the baseline conceptual framework for reasoning about privacy issues. We will then review privacy regulation (or more accurately, the lack thereof) in the US in comparison with the General Data Protection Directive (GDPR) that just came into effect in the EU. Like previous discussions, we will focus on the gap between policy objectives and the incentives of a transnational, decentralized cohort of private actors that are necessary to realize those objectives.

Like issues of privacy and surveillance, the decentralized character of the Internet also provides a wide variety of mechanisms for implementing censorship regimes and denying human rights online. In this lecture we will review the role of governments and the private sector combatting censorship. Broadening the discussion, we will discuss the issue of human rights and Internet access, debating whether Internet access itself is a human right or whether it is simply a tool that, following our earlier discussions of generativity, can be a tool to enable, or constrain, human rights.

Essential Readings

- **Nissenbaum, Helen (2004). "Privacy as Contextual Integrity''. In: *Washington Law Review* 79. https://heinonline.org/HOL/P?h=hein.journals/washlr79&i=129, pp. 119–158.**

- **Sowell, Jesse H. (2010). "Mixed Context and Privacy''. In: *Proceedings of the 38th Research Conference on Communication, Information and Internet Policy.***

- **Taddeo, Mariarosaria and Luciano Floridi (2016). "The Debate on the Moral Responsibilities of Online Service Providers''. In: *Science and Engineering Ethics* 22.6, pp. 1575–1603. DOI: 10.1007/s11948-015-9734-1.**

- **Joyce, Daniel (2015). "Internet Freedom and Human Rights''. In: *European Journal of International Law* 26.2, pp. 493–514. DOI: 10.1093/ejil/chv021.**

- **Zittrain, Jonathan L., Robert Faris, Helmi Noman, Justin Clark, Casey Tilton, and Ryan Morrison-Westphal (2017). *The Shifting Landscape of Global Internet Censorship.* SSRN Scholarly Paper ID 2993485. https://papers.ssrn.com/abstract=2993485. Rochester, NY: Social Science Research Network.**

- **Zalnieriute, Monika and Stefania Milan (2019). "Internet Architecture and Human Rights: Beyond the Human Rights Gap' '. In: *Policy & Internet* 11.1, pp. 6–15. DOI: 10.1002/poi3.200.**

Contemporary Readings

- **Cerf, Vinton G. (2012). "Internet Access Is Not a Human Right' '. In: *The New York Times*. https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.**

Optional Readings

- **Deibert, Ronald, John Palfrey, Rafal Rohozinski, Janice Gross Stein, Jonathan Zittrain, Robert Faris, Ernest J. Wilson III, and Nart Villeneuve (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. http://ebookcentral.proquest.com/lib/tamucs/detail.action?docID=3338769. Cambridge, UNITED STATES: MIT Press.**

  Read Chapters 1 and 2. Skim Chapter 3, 4, and the selected regions and countries that interest you.

Class #11: Tuesday 09 November 2021

Disinformation Campaigns

While we are now all familiar with the notion of disinformation from the debates around Russian interference in the 2016 elections, the notion of disinformation, and more broadly information warfare, has been around for 100s of years. In this lecture we will briefly survey and summarize the core literature on information warfare and disinformation. Next, we will review not only the 2016 issue, but the rise of disinformation-based strategies by various state and non-state actors attempting to replicate Russia's "success" story. Finally, we will conclude with a more sober analysis, highlighting that while the media focuses on substantive impacts ("successes"), these strategies are very hit-and-miss. Moreover, private actors are beoming more aggressive in curbing these campaigns. We will discuss these actions and, once again, revisit the necessity of public private partnerships in this space.

Essential Readings

- **Lazer, David M. J., Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts, and Jonathan L. Zittrain (2018). "The Science of Fake News' '. In: *Science* 359.6380, pp. 1094–1096. DOI: 10.1126/science.aao2998.**
- **Tandoc Jr., Edson C., Zheng Wei Lim, and Richard Ling (2018). "Defining 'Fake News" '. In: *Digital Journalism* 6.2, pp. 137–153. DOI: 10.1080/21670811.2017.1360143.**
- **Benkler, Yochai, Robert Faris, and Hal Roberts (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York, NY: Oxford University Press.**

  Skim most of Chapter 1, **read** the Sections *Definitions: Propaganda and Its Elements, Purposes, and Outcomes* (pp. 23–38). Skim Chapter 3, reading the first part on the *Propaganda Feedback Loop* (pp. 75–82). Read Chapters 7 and 8. Skim Chapter 10, Read Chapters 11 and 12.

Optional Readings

- **Ferrara, E., O. Varol, C Davis, F. Menczer, and A Flammini (2016). "The Rise of Social Bots' '. In: *Communications of the ACM* 59.96. https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext.**

- **Vosoughi, S, D Roy, and S Aral (2018). "The Spread of True and False News Online''. In: *Science 359*, pp. 11465–1151.**
- **Wu, Tim (2017). *The Attention Merchants: The Epic Scramble to Get Inside Our Heads.* Reprint edition. New York: Vintage.**
- **Benkler, Yochai, Robert Faris, and Hal Roberts (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.* New York, NY: Oxford University Press.**

Class #12: Tuesday 16 November 2021

Cybersecurity, Cybercrime, and Operations

As we know from the issues discussed thus far in Part II, many cyber policy issues require substantive public private collaboration to be effective. In this lecture we will roll up many of the issues we have discussed thus far under the umbrella of cybersecurity, how we protect both the infrastructure and end users (citizens from the perspective of state actors) from malicious activities online. We will review the history of cybercrime, how it evolved from the equivalent of online graffitti to a mature, ellicit market for malware (or cyberweapons in the next lecture), often referred to as crimeware as a service (CaaS). We will conclude this discussion by delving into some of Dr. Sowell's research on the challenges facing collaboration between private cybersecurity intelligence groups, law enforcement, and intelligence agencies. In this discuss we will cover the role (and failure of) mutual legal assistance treaties (MLATs) and recent cases that highlight the only way to combat cybercrime is through combining the capabilities of the state and the private sector.

Essential Readings

- **Anderson, Ross and Tyler Moore (2006). "The Economics of Information Security''. In: *Science* 314.5799. http://science.sciencemag.org/content/314/5799/610, pp. 610–613.**
- **The Rendon Group (2011). *Conficker Working Group: Lessons Learned.* http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/LessonsLearned. Rendon, VA: The Rendon Group.**
- **Vixie, Paul (2014). *Hearing on Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.* https://www.judiciary.senate.gov/imo/media/doc/07-15-14VixieTestimony.pdf. Washington, DC.**
- **Sowell, Jesse H. (2018). *Combining Capabilities in Cybersecurity Incident Response.* Stanford, CA: Center for International Security and Cooperation, Freeman Spogli Institute for International Studies, Stanford University.**

Contemporary Readings

- **FBI (2019). *Cyber Crime.* https://www.fbi.gov/investigate/cyber. Folder**
- **Interpol (2019). *Cybercrime.* https://www.interpol.int/en/Crimes/Cybercrime.**
- **FBI (2011). *International Cyber Ring That Infected Millions of Computers Dismantled.* https://www.fbi.gov/news/stories/international-cyber-ring-that-infected-millions-of-computers-dismantled. Story**
- **Krebs, Brian (2012). *Microsoft Responds to Critics Over Botnet Bruhaha.* https://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/.**
- **Greenberg, Andy (2018). "Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market''. In: *WIRED.* https://www.wired.com/story/hansa-dutch-police-sting-operation/.**

Class #13: Tuesday 23 November 2021

Cyberwarfare

What precisely constitutes cyberwarfare remains a contentious issue. In this lecture we will review existing definitions produced by state actors in work such as the Tallin Manual and the UN Group of Government Experts (GGE) (and the failure of this group's last meeting). Building on the work from the last lecture, we will highlight that while cyberwarfare is often distinguished from cybercrime, the very same tools and strategies, as well as a distinct set of highly skilled non-state actors, are often at play in both endeavors. Finally, we will conclude the discussion by exploring the classic notions of deterrence and coercion, in particular how the operationalizations of these concepts differ substantively from conventional notions of deterrence and coercion such as nuclear deterrence and limited warfare.

Essential Readings

- **Libicki, Martin C. (2009). *Cyberdeterrence and Cyberwar.* Rand Corporation.**

  Read Chapter 2 and 3.

- **Kello, Lucas (2013). "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft''. In: *International Security* 38.2, pp. 7–40. DOI: 10.1162/ISEC_a_00138.**

- **Lindsay, Jon R. and Lucas Kello (2014). "Correspondence: A Cyber Disagreement''. In: *INTERNATIONAL SECURITY* 39.2. http://proxy.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edspmu&AN=edspmu.S1531480414200052&site=eds-live, pp. 181–188.**

- **Kello, Lucas "Correspondence: A Cyber Disagreement Reply''. In: *INTERNATIONAL SECURITY* 39.2. http://proxy.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edswss&AN=000345522800007&site=eds-live, pp. 188–192.**

- **Lindsay, Jon R. (2015). "The Impact of China on Cybersecurity: Fiction and Friction''. In: *International Security* 39.3, pp. 7–47. DOI: 10.1162/ISEC_a_00189.**

- **Brenner, J. and J.R. Lindsay "Correspondence: Debating the Chinese Cyber Threat''. In: *International Security* 40.1, pp. 191–193. DOI: 10.1162/ISEC_c_00208.**

- **Lindsay, Jon R. (2015). "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack''. In: *Journal of Cybersecurity*, pp. 53–67. DOI: 10.1093/cybsec/tyv003.**

Class #14: Tuesday 30 November 2021

Project Presentations

In this class students will present their policy research projects.

Assignments and Writing Guidelines

The following provides details on the assignments for the course. All assignments *must be submitted in PDF format* and conform to the writing format guidelines. All assignments should be submitted electronically via Turnitin. All assignments are due *at or before 2359* on the assignment due date.

Assignments

As described briefly in Grading, course assignments comprise participation, a presentation of class readings, a take-home mid-term, a policy memo, and a policy research project. As a note on writing requirements, the length requirements are described in terms of *maximum* word count; there is no minimum. For the page equivalent, 500 words is *approximately* 1 page with 1 inch margins, **single-spaced**, 12 pt Times New Roman (or a very similar serifed font like the one used in this document).

Participation

Participation is made up of contributions in class (6 points) and peer-review of assignments (4 points). These are described below.

Class Contribution You will start with 6 (out of a possible 10) points. You are expected to have completed all of the readings for a given week before the class and be ready to discuss those readings in class. Portions of each class will be run seminar style, with the expectation that students discuss the concepts and issues at hand in a civil, constructive, yet rigorously analytic manner. This is your opportunity to gain points. If you attempt to participate and clearly demonstrate you have not done the related reading, you will definitely lose participation points. That said, informed, thoughtful, civil, and constructive disagreement with other students or Dr. Sowell is encouraged, especially when Dr. Sowell makes intentionally leading, biased, or contradictory assertions to encourage discussion and creativity.

Also, as a note on participation, Dr. Sowell realizes that laptops and tablets are the modern mechanisms for taking notes. Dr. Sowell also encourages students to quickly look up relevant materials online to contribute during discussion. **Please refrain from spending class time on e-mail, social media, instant messaging, or anything else that is not directly related to the class or discussion at hand.**

Peer Review For the policy project proposal, detailed outline, rough draft, and the policy memo, we will being doing a 20-30 minute peer review in the class the following week after the assignment is due. Each of these peer reviews will be worth 1 point of your final grade and will be submitted via Turnitin the *Monday* before our Wednesday class so Dr. Sowell and the recipient of the review can read over the peer reviews.

You will be paired with another student to peer review their assignment for writing and critical thinking. This means you are expected to read their work and provide a maximum 500 word, ***constructive critical assessment*** of how well they conveyed their ideas. This *is not* as summary of their assignment. You should describe what elements of the writing were effective, and more importantly, which could be improved upon based on the learning objectives for that assignment.

Class Presentations

Each student will be required to do *one* in-class presentation on materials from the essential readings for a selected class. The choice of the class and the reading from that class is up to the student. **Extra credit of up to 2 points** will be given if the student includes (and effectively uses) external references (i.e., news or journal articles *not* currently in the course materials available in the course's shared Zotero library) to support their discussion points.

A Google survey will be sent out after Class 01 for students to select the topic they wish to present on. The survey will be first come, first serve.

Guidelines For the presentation itself, the student will:

- develop a set of slides that walk the class through the selected topic
- create a folder (collection) in their shared group library on Zotero for their presentations
    - name presentations folder `Class Presentations`
    - within that folder, create a folder for each presentation the student is presenting entitled `lastname Class X Presentation` where `X` is the class number
    - add presentation slides to the corresponding folder
        - in PDF or
        - if using Google Slides, add the link and share with jsowell@tamu.edu
    - add references used in the slides to the corresponding folder
- the presentation is expected to run for a maximum of 10 minutes, *not including* discussion

- prepare **3** leading questions for discussion (which should be after your conclusions slide)
- send a note to Dr. Sowell by 0800 on the day of the presentation indicating the slides are in Zotero

The student may present either from the classroom PC or their own laptop. The student is strongly encouraged to test their setup at least a day before the date of their in-class presentation.

Class Presentation Schedule Students will be sent a form to select their preferences for presentation topics. The schedule of class presentations will added to `Syllabus` folder in Zotero after the schedule has been established.

Please send Dr. Sowell an e-mail indicating which paper you will be presenting for your class presentation *the Friday before* the week of your presentation.

Policy Memo

Assignment due: *Wednesday 08 December 2021* along with final draft of policy research project.

Learning Objectives:

- summarize *and evaluate* the policy and/or security issues presented in your policy research project for an audience at the policy making and/or executive level
- present the reader with well-defined options, without leading the reader
- compare and contrast options
- balance these options and offer a recommendation

Word count: between *500 and 1000 words*, approximately 1-2 pages.

It is common to read policy memos that simply summarize and organize well-known, high-level issues. They provide a very brief tour of a given issue, such as the "going dark" debate or network neutrality. The more compeling policy memo provides an analysis of an issue based on a substantive, deep dive into the material (such as your policy research project). You may choose one of two "styles" of policy memo: present options to the reader and let them decide or present options, and a solution. In either case, the presentation of material and options should be representative of the issue and factors involved—it should not read as just one side of the debate or a partisan argument. The policy memo should present the essential factors at play; evaluate their implications; provides very important, select illustrative instances; presents the options available; and may offer a solution.

Mid-Term

The mid-term will be distributed on **Tuesday 26 October 2021** and will be due **at or before 2359 on Sunday 07 November 2021**.

The objective of the mid-term is to write a few small essays that apply the concepts developed thus far in the class. These essays will be graded on clarity and mastery of the concepts. This latter, mastery of the concepts, means that the student not only provides a convincing narrative, but effectively explains and utilizes concepts from the class, such as how the attribution problem applies, to describe a problem, explain the problem, evaluate that problem, then prescribe effective policy and/or governance solutions.

Another role of the mid-term is to get feedback on structuring a sociotechnical analysis, one that integrates an understanding of the technical dynamics introduced in lectures and the policy and governance problems and implications that arise when the technical (inevitably) becomes political. The kind of analysis expected in the mid-term is practice for the kind of analysis expected in the policy research project described below.

Policy Research Project

The objective of the policy research project is for you to apply lessons and concepts learned in the course to a policy or governance issue area of the student's choice. You are expected to apply what you have learned about the Internet's function, the organizations and institutions managing these functions, how these actors cope with endemic uncertainty, and how these actors are learning to engage with conventional actors in the global political arena (states, international governmental organizations, non-governmental organizations, etc.). There is no minimum word limit, but the maximum word limit is 10,000 words, approximately 20 pages. See the writing guidelines for specifics on what does and does not contribute to the word count.

Students are *required* to maintain the references used in their assignments, in particular for the policy research project, in Zotero. If the student has not already, the student should create a Zotero account.

Policy research project milestones:

1. **Zotero Policy Research Project Group**

   Assignment due: ***Thursday 02 September 2021***

   Students will use Zotero to create a shared group (library) entitled `Z - CP - lastname - Final` (where `lastname` is your last name). The link to create groups is only available via the web interface, click on the `Groups` tab and then `Create A New Group`. Then use Zotero's group invitation function (under the `Manage Members` link below the name of the group in the list of groups) to invite Dr. Sowell (jsowell@tamu.edu) to the group. Under `Library Settings` the Zotero Group should be private and Dr. Sowell should have edit rights so he can share references with the student. **This task is worth 3 points of your final grade (from participation). If you do not set up and share your Zotero library by 2359 on Thursday 02 September 2021 you will lose these points permanently.** For step-by-step instructions, see the section on Zotero Configuration in the Appendix. If you have any questions or run into any problems, please e-mail Dr. Sowell (jsowell@tamu.edu) at least one hour before class on Thursday 02 September 2021.

   All references used in the policy research project *must* be saved in the student's shared Zotero library. This will make your life a lot easier: you can easily copy references from the course library to your library for use in your policy research project, it allows Dr. Sowell to review your policy research project references with you, and allows Dr. Sowell to share relevant references with you when appropriate. When adding references to journal articles, reports, etc., you should make sure the PDF of the document is attached to that entry. The Zotero Connector will often do this for you, but you should double check and add the PDF if it does not.

   Students will submit the milestone deliverables for their policy research projects (enumerated below) via Turnitin.

2. **Proposal** *(10%)*

   Assignment due: ***Friday 17 September 2021***

   Peer Review due: ***Monday 20 September 2021***

   Learning Objectives:

   - briefly summarize a cyber policy issue
   - describe the broad problem
   - narrow the issue to a policy research issue
   - describe the type of literature review and analysis that will help solve the narrower problem proposed

   The proposal should be a 500 word (max) description of the policy or governance issue the student will address in their policy research project. At a minimum, the proposal should reference readings from the course (with a bibliography that does not count against the 500 word limit). A *good* proposal will also include references to materials outside the course that (1) support the arguments in the proposal and (2) shows the student has already started their own research on the topic.

3. **Detailed Outline** *(15%)*

   Assignment due: ***Friday 22 October 2021)***

   Peer Review due: ***Monday 25 October 2021)***

This milestone has two parts: the detailed outline and a systematic literature review, which should be an appendix of your detailed outline document.

Learning Objectives:

- decompose the ideas for policy research in the proposal into distinct elements of an article (introduction, background, cases, analysis, recommendations, conclusions)
- understand how these contribute to and build into a well-researched and well-argued policy analysis
- use a detailed outline to map out the fundamental structure and flow of the paper's argument
- identify and incorporate additional research on your topic into the argument that is developed
- understand the role developing background concepts and uses those concepts in cases and as the connective logic in analyses and recommendations
- recognize that your argument **will iteratively change, evolve, and improve** over the course of the detailed outline, your drafts, and the final

The objective of the detailed outline is to articulate the fundamental structure of the project report, the current analysis and arguments, supporting materials, and how these are used to support the analysis and argument. The outline is intended to get the student thinking about the structure of the argument; it is expected to change based on feedback and further work leading up to the rough draft. That said, the detailed outline should articulate a clear and coherent narrative, argument, and supporting analysis.

There are two examples of detailed outlines from previous classes in the shared Zotero library under `Syllabus/Detailed Outline Examples`. Both of these received full credit and the admiration of Dr. Sowell for excellent work. The Hickman example follows the "syllabus model" criteria (described below) for a detailed outline. The detailed outline clearly lays out substantive openers and closers and clearly and articulately establishes the flow of the argument and supporting evidence. Hickman also provided excellent citations to back her assertions. The Burdette example uses the "quote method" for detailed outlines. This does include openers and closers, but provides nuance by integrating quotes and citations to sources that apply to that section (or subsection), demonstrates the flow of the argument, as well as the depth of the research on the project up to that point. Either of these models is acceptable.

The "syllabus model" of a detailed outline comprises:

- a title page (title, name, date)
- the approved proposal, followed by
- enumerated headers (1, 2.3, 5.6.3, etc.) for the major sections, subsections, etc.
- enumerated sections should include an "opener" and a "closer" that conveys the content for that section:
  - the overall objective of the detailed outline is to tell the high-level story of the argument and analysis
  - the "opener" (1-3 sentences) is like an opening paragraph: it introduces the topic, problem, argument, or analysis to be presented in that section
  - the "closer" (1-3 sentences) is like the concluding paragraph: it articulates the take-aways of a narrative, summary of the problem, highlights of the argument, or conclusions of an analysis
  - sentences in both the opener and closer should be substantive declaratives, **not** "This section will do this" or "This section will show that"
- an annotated bibliography
  - every work *you cite* in your project should have an annotation in the `Notes` section of the bibliographic entry in Zotero
  - each annotation of the bibliography should be two to three sentences, describing how this work contributes to the background, analysis, and/or argument
  - add your annotations to the `Notes` section of the Zotero bibliographic entry for each work you cite in your project, it does not have to be in the report itself

4. **In Class Project Presentation** *(5%)*

Assignment due *Tuesday 30 November 2021*

Learning Objectives:

- succinctly convey the key elements of your work in a way that can be understood *without* reading your entire paper
- recognize a presentation will not necessarily incorporate all of your findings
- recognize that the presentation may not have the same structure (major sections) as your paper
- understand the value of writing a script for your presentation, but *not reading from that script* in the presentation itself
- effective use of bulleted points to guide the presentation, but only selectively use long sentences or quotes
- appropriate use of visuals such as images, graphs, or diagrams to keep the audience's attention and drive home points, but not overwhelm the audience with distractions

On the last day of class students will present their policy research projects. Each student presentation will be approximately 15 minutes followed by discussion. Slides are required for the presentation.

5. **Policy Research Project Report** *(20%)*

Assignment due: *Wednesday 08 December 2021*

Learning Objectives:

- no piece of writing is *ever* perfect and you will always find ways to improve it
- identify elements of your rough draft that need additional detail
- identify elements of your rough draft that were redundant, or that you thought would contribute to your argument but are not as important as you thought—it is OK to delete unnecessary material as it distracts from an effective overall argument and recommendations
- identify insights from writing in later sections (cases, analyses, recommendations) that can be summarized and moved into earlier sections (introduction, background) to effectively signpost your argument, making the flow more effective and guiding the reader through your argument
- write a 500 word maximum executive summary of the final report that summarizes the problem, the background concepts and issues at play, the cases, your analysis, and your recommendations; this should not just be a variation of your introduction, but rather a concise articulation of the key points for a policy maker, regulator, or exective that wants to know whether this is worth digging into further (or having their staff dig into this work further)
- know when to (perhaps thankfully) stop revising

Policy research project reports will follow the write-up formatting guidelines below.

Write-Up Formatting Guidelines

These guidelines are not optional and will be strictly enforced. If you submit material that does not conform to these guidelines, it will be returned ungraded and with a 10% late penalty.

- single-spaced
- title page with title, name of author, and date; title page should not have a page number
- title page does not contribute to word count for assignment unless otherwise specified
- executive summary (where required in the project specification) should be on the page following the title page, introduction to paper should start at beginning of following page
- font should be New Times Roman or similar serifed font
- font size for executive summaries and body of text should be 12 pt
- document should be fully justified as in books and journal articles, no ragged right edge
- use enumerated footnotes, 10 pt; *do not ever use endnotes*
- 1 inch margins all around (left, right, top, bottom, this is standard in Word)
- block quotes consistently inset from left and right margins
- page enumeration in footer, no page number on title page, body enumeration starts starts at page 2
- enumerate sections and subsections (1, 2.1, 3.5.2, etc.)

- figures should be labeled ("Figure 1: Scatter plot of data set X", "Figure 2: Distribution of variables in category Y", etc.), referenced by figure number ("Note that the distribution in Figure 4 is left skewed. . . "); figure labels will contribute to word count
- references must be stored in Zotero
- in-text references and bibliography should follow *Chicago Manual of Style 17th Edition (author-date)* format, you can find this in the Zotero settings under `Cite`.
- the bibliography will not contribute to the word count
- in-text references:
  - materials (articles, books, etc.) with page numbers must include the page number or page range that includes the quote or evidence referenced
  - materials, such as web pages that are not enumerated, should include the finest grained subsection containing the quote or evidence where the page number or page range would be in the in-text reference
  - in-text references that do not follow these guidelines will result in assignment returned with a 10% penalty
- documents submitted should be in PDF format and should allow highlighting of text using PDF annotation tools such as Adobe Acrobat Reader; you should check this as you write and before submitting, exotic invisible formatting in Word occasionally breaks this requirement
- PDF documents will be submitted electronically via Turnitin; hard copy will not be accepted

Dr. Sowell will provide an example PDF to illustrate these guidelines. When grading your assignments, Dr. Sowell will annotate your document electronically. Any mainstream PDF reader, such as Adobe Acrobat Reader, Skim, or Apple's Preview will render these comments. A comment attached to the upper left of the title page or first page of the assignment will contain the total grade and overall comments. Annotated PDFs with your grades will be uploaded to your Zotero shared library.

University Policies

Attendance

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Other absences may be excused at the discretion of the instructor with prior notification and proper documentation. In cases where prior notification is not feasible (e.g., accident or emergency) the student must provide notification by the end of the second working day after the absence, including an explanation of why notice could not be sent prior to the class.

On some occasions, the instructor may have to miss a class due to administrative or academic responsibilities out of town. If it does occur, the instructor reserves the right to reschedule class at a time when the vast majority of students are available for the make-up class and will convey the material to students unable to attend the make-up during office hours.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student's grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

"Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor" (Student Rule 7, Section 7.4.1).

"The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence" (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code (see Student Rule 24).

Academic Integrity Statement and Policy

"An Aggie does not lie, cheat or steal or tolerate those who do."

"Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one's work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case" (Section 20.1.2.3, Student Rule 20).

You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

Dr. Sowell strongly encourages reading groups for discussing course materials, but not for distributing the reading load. Dr. Sowell also recognizes the role and efficacy of group learning and peer review of assignment deliverables, such as proof-reading one another's work and/or discussing the structure and flow of arguments presented in assignments. If you engage in this kind of collaboration, you must add a footnote to the your name (as the author) with a statement indicating who you collaborated with and how they contributed to the work you are turning in under your name. As an example, "John Smith proof-read a draft of this assignment, providing editorial comments and suggesting I rearrange the order of my cases to improve the logical flow of my case studies section." Another example would be "I discussed this assignment with Jane Smith and she suggested the articles (Warner 2016; Billings 1967), which I have included in this work."

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact Disability Resources in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu. Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

Title IX and Statements on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see University Rule 08.01.01.M1):

- The incident is reasonably believed to be discrimination or harassment.
- The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written class assignment or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, you will be able to control how the report is handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with Counseling and Psychological Services (CAPS).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in proper self-care by utilizing the resources and services available from Counseling & Psychological Services (CAPS). Students who need someone to talk to can call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Appendix

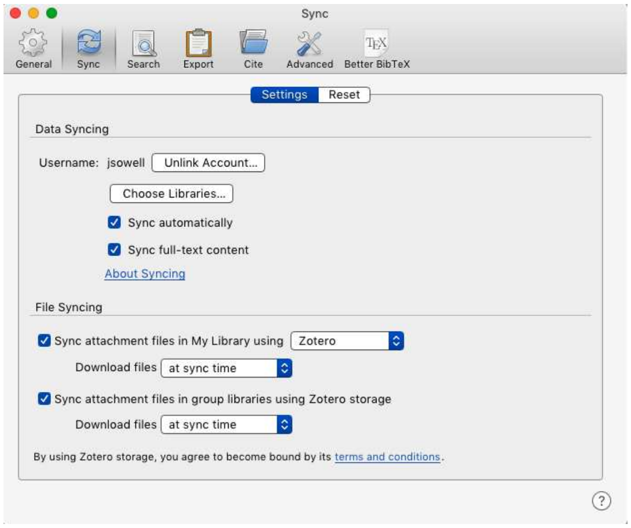
Zotero Configuration

The following instructions describe how to set up the Zotero App and create a shared group library.

Zotero App Setup

1. Create a Zotero account at https://www.zotero.org using your `@tamu.edu` e-mail address.
2. Install
   1. Zotero app, available at https://www.zotero.org/download/
   2. Install the Zotero Connector web browser plugin, available at https://www.zotero.org/download/connectors
3. You should receive an invitation to the course library in both the e-mail you set up your account with and in the Zotero Inbox, available via the Zotero web interface.
4. To confirm your Zotero app is syncing with the course library, you should check your Zotero app preferences. In the `Preferences` window, select the `Sync` tab and confirm that
   - Zotero shows `Username: your_username` (where `your_username` is your username)
   - you have checked `Sync Automatically` and `Sync full-text content`
   - you have checked `Sync attachment files in My Library using Zotero` and selected `Download files at sync time`
   - you have checked `Sync attachment files in gorup libraries using Zotero storage` and selected `Download files at sync time`

   A screenshot illustrating what your settings should look like can be found below.



Data Syncing

Username: jsowell

☑ Sync automatically

☑ Sync full-text content

About Syncing

File Syncing

☑ Sync attachment files in My Library using Zotero

Download files at sync time

☑ Sync attachment files in group libraries using Zotero storage

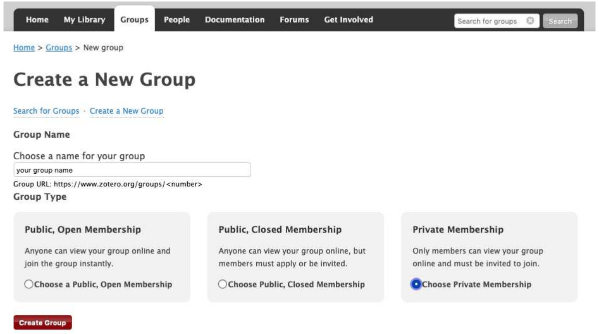
Download files at sync time

By using Zotero storage, you agree to become bound by its terms and conditions.

If you prefer not to sync automatically, uncheck `Sync automatically`. ***If you choose this option you will have to explicitly sync your libraries using the small circular green arrow in the upper right of the Zotero app.***

Shared Groups (Library) Setup

1. Log in to the Zotero web interface at https://www.zotero.org
2. Click on the `Groups` link
3. Click `Create a New Group` link directly under the header `Zotero Groups`
4. Add a name for your shared library where it says `Choose a name for your group` and select the `Group Type` as `Private Membership` as illustrated below



Create a New Group

Group Name

Choose a name for your group

your group name

Group URL: https://www.zotero.org/groups/<number>

Group Type

Public, Open Membership

Anyone can view your group online and join the group instantly.

○ Choose a Public, Open Membership

Public, Closed Membership

Anyone can view your group online, but members must apply or be invited.

○ Choose Public, Closed Membership

Private Membership

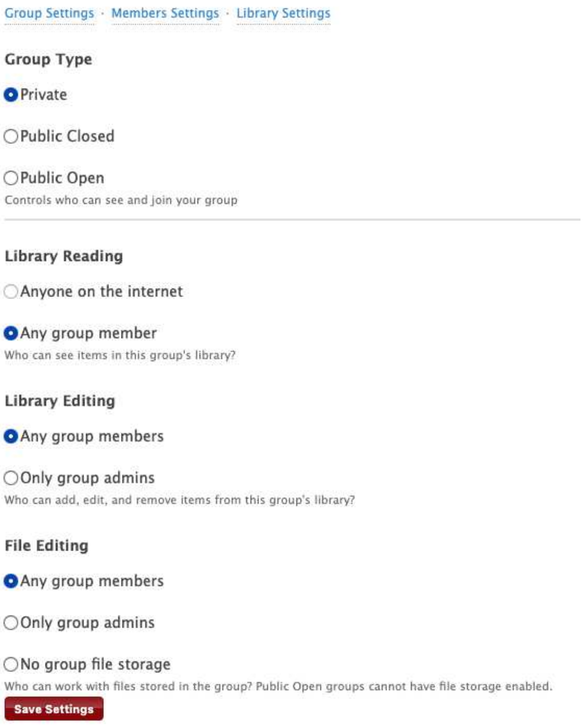
Only members can view your group online and must be invited to join.

● Choose Private Membership

5. Click the `Create Group` button
6. Select the following group settings (illustrated in the screenshot below):

   – for `Group Type`, select `Private`
   – for `Library Reading`, select `Any group member`
   – for `Library Editing`, select `Any group members`
   – for `File Editing`, select `Any gorup members`

   then click `Save Settings`; these are the defaults, so you should not have to change anything.



Group Settings · Members Settings · Library Settings

Group Type

● Private

○ Public Closed

○ Public Open

Controls who can see and join your group

Library Reading

○ Anyone on the internet

● Any group member

Who can see items in this group's library?

Library Editing

● Any group members

○ Only group admins

Who can add, edit, and remove items from this group's library?

File Editing

● Any group members

○ Only group admins

○ No group file storage

Who can work with files stored in the group? Public Open groups cannot have file storage enabled.

7. To add new members to the group, click the blue link `Member Settings` link under the heading `groupname: Member Settings` and click the link `Send More Invitations` at the bottom of the page and follow the instructions there.

Notes on Zotero Connector Plugin

The Zotero Connector adds a small icon to the right of the address bar in your web browser (upper right corner of the window). To use the Connector, the Zotero app must be open. By default, when you click the Zotero icon to download a given reference, it will automatically put that reference *in whichever folder you currently have selected in the Zotero app.* This is quite convenient if you have organized your research folder into topic specific subfolders, or, in my case, if you have it organized by class and category of reading material (essential, optional, etc.).

INTA 708 - Data Science and Visualization for Policy Analysis

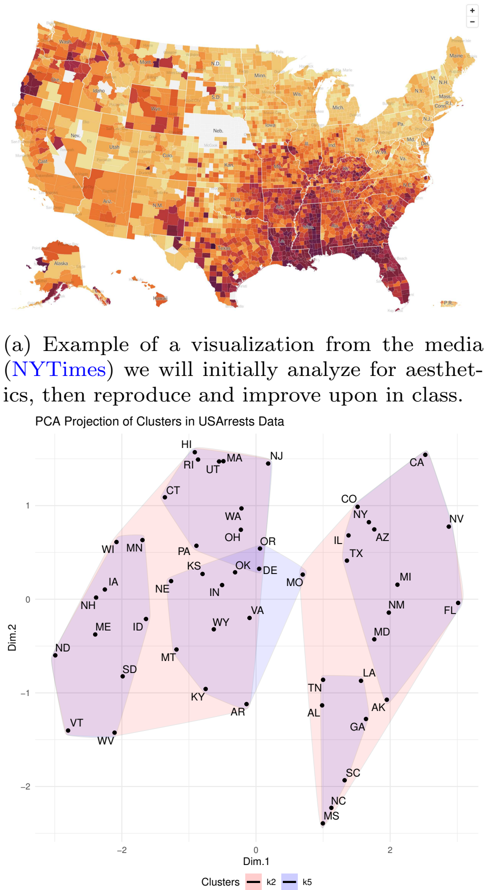
Wednesdays, 1330-1620 in Allen 1055 with Dr. Jesse Sowell

No prerequisites, ***designed for students with little to no coding experience***

All texts, readings, and software for this course are freely available online

Modern policy analysts are faced with developing a compelling visual narrative from a surfeit of data. This course will equip you with the data science skills necessary to make sense of our increasingly data rich policy environment. Data science and visualization provides the tools for cleaning, integrating, and transforming this data into a form that can be tractably evaluated and effectively visualized. This course focuses on data management and exploratory data analysis (EDA) tools for hypothesis generation through an applied introduction to mapping, cluster analysis and principal component analysis, social network analysis, and text mining. The policy research project is structured for you to choose *your own* data adventure by delving into a policy issue and data sets that further your academic and professional interests and development. Previous projects have focused on cybersecurity, international trade flows and economic development, treaty networks, terrorism, water policy, performance of non-profits, hospital resource allocation, public procurement, comparative agriculture policy, and China's foreign policy, to name a few.

Starting with exploratory analyses driven by data visualization, you will develop and iteratively apply the data science skills and workflows necessary to identify and develop compelling visualizations of trends in your policy area, culminating in a final policy research project and analysis portfolio. At the end of this course, you will have established a strong foundation in data management and data science, *and* a portfolio of analyses and visualizations that previous students have used to provide compelling illustrations of their skills to potential employers.



(a) Example of a visualization from the media (NYTimes) we will initially analyze for aesthetics, then reproduce and improve upon in class.

(b) Visualization of a clustering and principal components analysis we work through in class.

Figure 1: Illustrations of analyses and visualizations used in class that you will learn how to design, adapt, interpret, and analyze.

Course Structure

This project-based course (no exams!) develops concepts and skills through learning exercises, then applying these to your policy research project. Part I of the course introduces aesthetic strategies for developing compelling, meaningful visualizations, and how these concepts are used for hypothesis generation. The introduction also develops fundamental R, data management, data set integration (such as incorporating US Census and American Community Survey data), and data transformation skills. Throughout the course, skills are illustrated in class with small well-understood data sets, then applied to live data such as the NYTimes' COVID-19 data to create, critique, and improve on visualizations such as those in Panel 1a. Part II focuses on EDA and cluster analyses to help you understand the nuance of observed trends and outliers (such as in Panel 1b), which observations and variables contribute to different kinds of clusters, ultimately laying the foundation for effective "storytelling with data." The remainder of the course integrates the fundamentals of common data science and visualization tools and methods: mapping, social network analysis, and text mining.

The best way to learn data science is through practice with pragmatic examples. Learning exercises give you the opportunity to work through variants of in-class examples individually *or in groups.* In your policy research project, you will apply these concepts and tools to a policy issue salient to your career path. Project milestones are structured to iteratively guide you through common data science workflows, helping you systematically work through the data cleaning, management, transformation, and visualization phases of your project. In addition to developing your data science skills, these milestones are structured to facilitate developing an analysis and visualization portfolio that effectively illustrates your analysis and understanding of the topic area you have selected. Previous students have used this course to work on topics that further their career development, topics and data for research projects they are already working on, and/or data from organizations and agencies supporting their studies. Recent graduates have indicated interviewers were quite impressed with their project portfolios.

If you have any questions about this course, please do not hesitate to contact Dr. Sowell at jsowell@tamu.edu. The current syllabus is available upon request.

Data Science and Visualization for Policy Analysis
INTA 708

Fall 2021
Wednesdays 1330 - 1620
1055 Allen Building

Instructor: Jesse H. Sowell II
E-mail: jsowell@tamu.edu
Office: 1096 Allen Building
Office Hours: Tuesdays 1630 - 1800 by appointment

Course Description

For many policy issues—in particular those at the intersection of science, technology, and public policy—the analyst is faced with a surfeit of data and the challenge of transforming this data into a form that can be tractibly evaluated. This course equips students with the data science skills necessary to make sense of our increasingly data rich policy environment. Starting with exploratory analysis driven by data visualization, students will develop the skills and workflows necessary to identify and develop compelling visualizations of trends in domestic and transnational policy issues.

As per our primary text (Wickham, 2017), data analysis falls into two general groups: hypothesis *generation* and hypothesis *confirmation*. This course focuses on data science and visualization for hypothesis *generation*. Part I focuses on what is colloquially referred to as "data wrangling": importing, cleaning, and integrating data from a variety of sources. Part II introduces the fundamentals of exploratory data analysis (EDA), visualization tools, mapping (basic GIS), and clustering, concluding with text mining. Following the theme of this course, we focus on how to use, interpret, and visualize analyses generated using these tools and strategies.

Course Schedule Overview

Week	Date	Lecture
01	01 September 2021	Introduction to Data Science for Policy Analysis
02	08 September 2021	Introduction to R
03	15 September 2021	Cleaning, Transforming, Managing Your Data
04	22 September 2021	Grammar of Graphics I
05	29 September 2021	Grammar of Graphics II
06	06 October 2021	Exploratory Data Analysis
07	13 October 2021	Reading Week
08	20 October 2021	Exploratory Data Analysis II
09	27 October 2021	Mapping
10	03 November 2021	Cluster Analysis I
11	10 November 2021	Cluster Analysis II
12	17 November 2021	Text Mining I
13	24 November 2021	Thanksgiving
14	01 December 2021	Text Mining II
15	08 December 2021	Project Presentations

Course Prerequisites

There are no prerequisites for this course. A background in basic statistics is strongly recommended.

Course Learning Outcomes

- understand the philosophy of data science applied to exploratory data analysis (EDA) and hypothesis *generation*
- apply this philosophy to a mixed methods approach to data science and visualization
- master data management skills, in particular the extract, load, transform (ELT) process
- understand the core principles of "data wrangling" using the principles of data transforms and the attendant tools in the `tidyverse` family of packages
- be able to evaluate visualizations in the media in terms of mapping data to aesthetics, as presented by Healy
- understand the principles of the grammar of graphics and apply these to develop visualizations
- understand and develop diagnostic, analytic, and public facing visualizations
- apply data transformations and visualization tools to perform common EDAs such as evaluating common aggregate indicators (measures of centrality and distributions) and develop dataset specific EDAs
- develop basic geographic information system (GIS) and mapping skills that build on the application of data aesthetics and the grammar of graphics to evaluate and visualize spatial trends
- understand the principles behind common clustering algorithms (k-means and hierarchical), how these facilitate identifying trends, patterns, and groupings of observations
- apply clustering to both quantitative and categorical variables
- understand how to apply, compare, and evaluate the results of different clustering strategies, and the kinds of groups that can be identified by those strategies
- apply principle component analysis (PCA) to reduce the dimensionality of clusters and effectively visually inspect, compare, and analyze groups identified by various cluster analyses
- use text mining and the principles of clustering to evaluate groups of text documents (corpi) for trends in concepts and sentiment
- use frequency and network analysis to better understand the relationships between concepts within and across corpi

Textbooks and Resource Materials

Books

Required

Each of these texts are freely available online or will be provided as PDF in the Zotero course library.

Grolemund, Garrett (2014). *Hands-On Programming with R: Write Your Own Functions and Simulations*. 1 edition. https://learning.oreilly.com/library/view/hands-on-programming-with/9781449359089/. O'Reilly Media.

Healy, Kieran (2018). *Data Visualization: A Practical Introduction*. 1st edition. https://socviz.co/. Princeton, NJ: Princeton University Press.

Lindgren, Simon (2020). *Data Theory: Interpretive Sociology and Computational Methods*. https://www.amazon.com/Data-Theory-Interpretive-Sociology-Computational-ebook-dp-B08HCGBH9L/dp/B08HCGBH9L/. Wiley.

Silge, Julia and David Robinson (2017). *Text Mining with R: A Tidy Approach*. 1st edition. https://www.tidytextmining.com/. O'Reilly Media.

Wickham, Hadley and Garrett Grolemund (2017). *R for Data Science: Import, Tidy, Transform, Visualize, and Model Data*. 1st edition. https://r4ds.had.co.nz/. O'Reilly Media.

References

The following are optional reference materials, some of which will be used as source materials for lectures.

Bruce, Peter, Andrew Bruce, and Peter Gedeck (2020). *Practical Statistics for Data Scientists, 2nd Edition*. Second. https://learning.oreilly.com/library/view/practical-statistics-for/9781492072935/. O'Reilly Media. *(electronic version available from library)*

Dalgaard, Peter (2002). *Introductory Statistics with R*. New York, NY: Springer. *(electronic version available from library)*

Engel, Claudia A. (2019). *Using Spatial Data with R*. https://cengel.github.io/R-spatial/. *(in Zotero, available online)*

Imai, Kosuke (2018). *Quantitative Social Science: An Introduction*. Princeton: Princeton University Press. *(PSEL library reserve, Dr. Sowell also has a copy)*

(in Zotero, available online)

Peng, Roger D. (2016). *Exploratory Data Analysis with R*. https://bookdown.org/rdpeng/exdata/. *(in Zotero, available online)*

(in Zotero)

Xie, Yihui, J. J. Allaire, and Garrett Grolemund (2019). *R Markdown: The Definitive Guide*. https://bookdown.org/yihui/rmarkdown/. CRC Press. *(in Zotero, available online)*

Xie, Yihui, Christophe Dervieux, and Emily Riederer (2021). *R Markdown Cookbook*. https://bookdown.org/yihui/rmarkdown-cookbook/. *(in Zotero, available online)*

Course Tools

The following course tools should be installed **before** the first lecture on Wednesday 01 September 2021.

R and RStudio

We will be using R and RStudio for data analysis and visualization. You will need to download and install the following applications to complete the assignments in this course.

1. R at https://cran.revolutionanalytics.com/
2. RStudio at https://www.rstudio.com/products/rstudio/download/#download

Students should install these applications in the order above. Please be sure to install these tools before the first class. We will be using RStudio extensively in each class to demonstrate various tools, methods, and visualization techniques. We will introduce some of the foundations of using RStudio in the first lecture, introducing additional skills and tools as the course progresses.

Zotero

We will be using Zotero to access course materials and to manage the references used in the course assignments. Unless otherwise indicated, students can find any of the materials listed on this syllabus (with the exception of some of the textbooks above) in the shared Zotero library for this course. These materials include journal articles, conference papers, newspaper and magazine articles, **lecture slides**, and **the most up-to-date version of this syllabus**. Dr. Sowell will be sending invitations to the Zotero shared library after the first lecture, the afternoon of Wednesday 01 September 2021. If the student has not received an invitation to the shared library, check your spam folder. If the student still cannot find the invitation, e-mail Dr. Sowell (jsowell@tamu.edu).

The first step to using Zotero is to create a Zotero account. Students can download the Zotero app at https://www.zotero.org/download/. Students should also install the Zotero Connector for the browser of their choice. For step-by-step instructions, see the section on Zotero Configuration in the Appendix. Word processor plugins are available for Word, LibreOffice, and Google Docs. That said, in this course we will be doing all the write-ups in Rmarkdown, so you will not need these.

TAMU libraries offers extensive documentation and tutorials on using Zotero. Please see:

- TAMU Zotero Research Guide
- Creating Bibliographies, in particular, the *two-minute* video that shows how to insert in-text citations into a Word document and how to generate bibliographies.
- The *less than two-minute* quick guide video for saving citations from your web browser

It should take less than 30 minutes to get the Zotero app and connector installed, setup, and then run through the two video guides. This will save you many more hours fiddling with references when writing your policy research projects.

Finally, to incorporate references into your mini-project and policy research project submissions, you will need to install the Zotero plugin Better BibTeX. It looks very technical, but you can ignore that for now. You can find the link for installing Better BibTeX at https://retorque.re/zotero-better-bibtex/installation/. We will work through the nuance of configuration in lecture.

Lecture slides will be added to the shared library at latest one hour before each class. The syllabus and class readings will be periodically updated with contemporary readings from the news related to upcoming topics in the course. To ensure you have the latest syllabus, it is strongly suggested that you open the syllabus directly from Zotero.

To be clear on the locations of these materials:

- the latest syllabus can always be found in the directory `INTA 689 - Data Science/Syllabus` (Zotero calls directories *collections*) of the shared library
- slides will be in the collection `INTA 689 - Data Science/Classes/ClassX/Slides` where `X` is the class number (01, 08, 12, etc.)
- references in slides that are not from one of the assigned books or one of the readings lists, can also be found in the `Slides` collection for that lecture

Please contact Dr. Sowell (jsowell@tamu.edu) if you have any problems accessing Zotero or the class materials in the shared library INTA 689 - Data Science.

GitHub

We will be using Github for your projects and assignments. In terms of software, students should

1. create a GitHub account using their `@tamu.edu` e-mail address
2. download GitHub Desktop, install it, and log into their GitHub account with the app

In the first class we will do a brief tutorial on how students will use GitHub to manage their policy research projects and learning exercises.

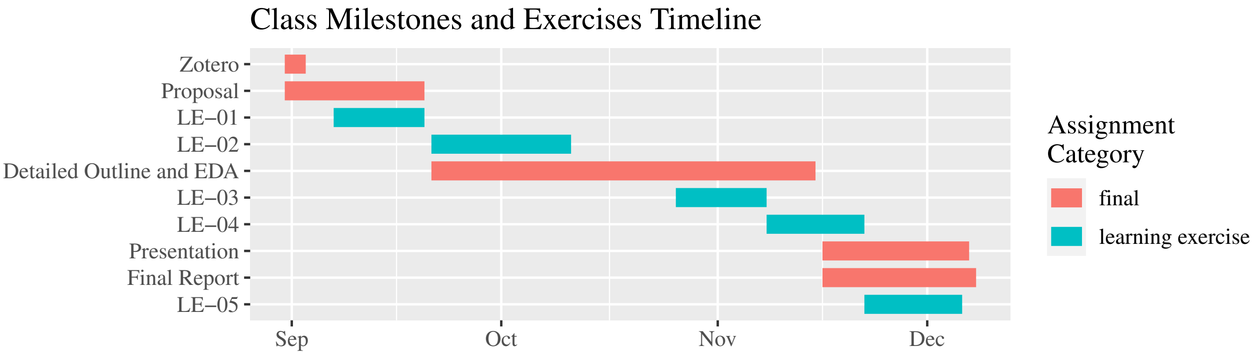
All project milestones and learning exercises for this course will be submitted via GitHub.

Grading Policy and Overview of Assignments

This is a project-based course, there are no exams. Details and guidelines for each assignment are provided in the Assignments section. Final grades will be calculated as follows:

1. participation, 10%
2. learning exercises, 30%
   - LE-01, Learning R, *due Monday 20 September 2021*
   - LE-02, Transforms, *due Monday 11 October 2021*
   - LE-03, Visualization and EDA, *due Monday 08 November 2021*
   - LE-04, Clustering, *due Monday 22 November 2021*
   - LE-05, Mapping, *due Monday 06 December 2021*

3. policy research project, total 60%, breakdown:
   - setup shared policy research project library in Zotero, 3 *participation points, due Friday 03 September 2021*
   - proposal, 5%, *due Monday 20 September 2021*
   - detailed outline and exploratory data analysis, 20%, *due Monday 15 November 2021*
   - in class presentation, 5%, *due Tuesday 07 December 2021*
   - policy research project report, 30%, *due Wednesday 08 December 2021*



Grades for assignments will be in terms of total points for the class. For instance, a good grade for the proposal would be 4.75/5.

Final letter grades will be assigned as follows:

letter grade	range
A	>= 90%
B	>= 80%, < 90%
C	>= 70%, < 80%
F	< 70%

In terms of evaluation, grades for project milestones (within the scope of the assignment) are assessed as follows:

- **A+, >= 96%** indicates
  - exceptional mastery of concepts at hand,
  - exceptional application of the concepts,
  - salient issues and concepts covered in the class are addressed,
  - appropriate trade-offs are discussed,
  - analysis is supplemented by contemporary instances of the problem from outside materials,
  - exceptional articulation, with an introduction to the problem, challenges, trade-offs, and recommendations where requested
- **A, >= 90%, <96%** indicates
  - accurate articulation of concepts at hand,
  - effective applicatin of the concepts,
  - *most* salient issues and concepts covered in the class are addressed,
  - appropriate trade-offs are discussed,
  - good articulation of the analysis with an introduction to the problem, challenges, trade-offs, and recommendations where requested
- **B, >= 80%, < 90%** indicates
  - accurate articulation of the concepts at hand,
  - effective application of the concepts,
  - only *some* key issues and concepts related the problem at hand are presented,
  - some trade-offs discussed in class are missing,
  - weak articulation of analysis, has only rudimentary introduction to the problem, challenges, trade-offs, and recommendations where requested
- **C, >= 70%, < 80%** indicates

  - inaccurate articulation of the concepts at hand,
  - weak or unclear application of the concepts,
  - significant key issues and concepts related to the problem at hand are missing or misconstrued,
  - limited discussion of trade-offs,
  - poor articulation of analysis, does not have a clear introduction to the problem, challenges, trade-offs, and recommendations where requested
- **F, < 70%** indicates
  - inaccurate representation of the concepts at hand,
  - little to no application of the concepts,
  - signifiant number of the key issues and concepts related to the problem at hand are missing or misconstrued,
  - very little discussion of trade-offs or single-sided,
  - writing is unclear and unstructured

Specific criteria for individual milestones can be found in the assignment descriptions.

Each set of learning exercises has an assigned point value. Each problem within the learning exercises has a clearly indicated point value. Learning exercises are evaluated in terms of the completeness and correctness of the solution to each problem. If no solution is offered, that problem is assessed at zero points. Partial solutions will garner points for that problem based on how complete and correct the solution is. Correct solutions (not always exactly the same as the solution) will garner all the points for that problem.

Late Work Policy

Enforcement of the following late work policy is at the discretion of the instructor.

As noted in the discussion of GitHub, *all assignments for this class are due at or before 2359 on the due date for the assignment.* **Late submissions will incur a penalty of 10% per day after the due date.** For instance, if the assignment is due on Monday and it is submitted on Wednesday, a 20% late penalty will be applied. *Assignments submitted on or after the tenth day after the deadline will receive zero points and will not be graded.*

Ideally, everyone plans ahead and gets work done ahead of time. That said, every student gets one *late submission mulligan.* Everyone gets behind at some point or finds they have several deliverables due at the same time and needs a little slack. If you see yourself heading for this situation, to use your mulligan you must e-mail the instructor *at least 24 hours before the deadline* to indicate you would like to take your mulligan, explain why, and when you think you can submit the work. The instructor will work with you to identify a reasonable revised deadline. You will likely get a day or two more time, a week is unacceptable with the exception of dire circumstances. *Like the overall late policy, the mulligan is also at the discretion of the instructor, so please do not abuse this generous option.*

Course Schedule: Lectures and Readings

All of the assigned textbooks, journal articles, papers, newspaper articles, and other documents assigned in the reading lists below can be found in the shared Zotero library for this course. Lecture slides will be added to the appropriate Zotero shared folder at latest one hour before class.

For any given class there will be at most three readings lists:

- **Essential Readings** are the *required* readings from the textbooks and course materials.
- **Contemporary Readings** are *strongly recommended* after reading the essential readings.
- **Optional Readings** are *not required.* These readings may be referenced in lectures. Optional readings may also be useful starting points for policy research project research.

Class #01: Wednesday 01 September 2021

Introduction to Data Science for Policy Analysis

In this lecture we will discuss the course objectives, get a feel for where each student is in terms of experience with data analysis and statistics, and review the course timeline and objectives. We will briefly review the difference between hypothesis generation versus hypothesis validation—this class largely about data science and visualization in support of hypothesis *generation*, although those with a sufficient background may incorporate validation into their projects. In the second half of the class we will introduce the tools we will be using in the class: the concepts and principles behind analysis in R, RStudio as the primary analysis tool, and RMarkdown as the tool for literate, reproducible research.

Essential Readings

- **Numanović, Amar (2017).** ***Data Science: The Next Frontier for Data-Driven Policy Making?*** **https://medium.com/@numanovicamar/https-medium-com-numanovicamar-data-science-the-next-frontier-for-data-driven-policy-making-8abe98159748.**
- **Wang, Joan (2017).** ***Musings at the Intersection of Data Science and Public Policy.*** **https://towardsdatascience.com/musings-at-the-intersection-of-data-science-and-public-policy-cf0bb2fadc01.**

Part I: Data Wrangling

Class #02: Wednesday 08 September 2021

Introduction to R

Data Science is about exploration and prediction. In this first half of this class, we will focus on exploration, in particular, methods and strategies for hypothesis *generation*. In this class we will provide an overview of the difference and relationship between hypothesis generation and confirmation and how these different strategies contribute to policy analysis. We will illustrate the concepts with instances we will explore in depth in class. In this class we will also introduce the basics of R: types of variables, how data is stored in R. We will illustrate these concepts through numerous examples from the text and the class datasets.

Essential Readings

- **Gastner, Michael T. (2021).** ***Data Analysis and Visualisation with R.*** **http://michaelgastner.com/DAVisR2021/.**

  Read Chapters 2; 3; Chapter 8, Sections 8.1(http://michaelgastner.com/DAVisR2021/chap-packages.html#installing-a-package) and 8.2; Section Section 4.1; Chapters 11 and 12.

  Gastner provides an excellent introduction to RStudio (Chapter 2), along with an introduction to the basic data types such as vectors (Chapter 3) and factors (Chapter 12). Factors are always one of the most challenging of the basic types for students to get used to, so you should spend some time to make sure you understand how they work.

- **Wickham, Hadley and Garrett Grolemund (2017).** ***R for Data Science: Import, Tidy, Transform, Visualize, and Model Data.*** **1st edition. https://r4ds.had.co.nz/. O'Reilly Media.**

  Read Chapters 1, 2, and 4.

  These Chapters introduce you to some of the language used in Wickham and some of the principles of data science. We will return to the data science workflows introduced in these chapters throughout the course.

- **Healy, Kieran (2018).** ***Data Visualization: A Practical Introduction.*** **1st edition. https://socviz.co/. Princeton, NJ: Princeton University Press.**

Read Chapter 2, Appendix 1.

Pay special attention to Section 2.4, be patient and realize the only way to become effective with these tools is practice.

- **Wickham, Hadley and Garrett Grolemund (2017).** ***R for Data Science: Import, Tidy, Transform, Visualize, and Model Data.*** **1st edition. https://r4ds.had.co.nz/. O'Reilly Media.**

  Read Chapter 27.

  This chapter introduces you to RMarkdown. As Wickham highlights, the best way to learn is to play with a few documents and try things out. All of your learning exercises and your policy research project are in RMarkdown, so you will have plenty of additional opportunities to apply these skills. This chapter should also serve as your reference to RMarkdown.

- **Cone, Matt (2019).** ***Markdown Guide: Basic Syntax.*** **https://www.markdownguide.org/basic-syntax/.**

  This is the foundational syntax for RMarkdown, the tool we will be using to create easily and systematically reproducible notebooks and reports. We will walk through some simple examples to get you started in the second half of lecture.

Optional Readings

- **Gastner, Michael T. (2021).** ***Data Analysis and Visualisation with R.*** **http://michaelgastner.com/DAVisR2021/.**

  Read Chapter 15.

  We will go over how to read data from `.csv`, `.xls[x]` files, and from Google Sheets in the class slides, but if you would like a reference, see Gastner, Chapter 15. This is assigned reading for the next class, but included here if you want to jump ahead a smidge.

- **Ramirez, Rebecca (2020).** ***The Science Behind Storytelling.*** **https://www.npr.org/2020/08/18/903545336/the-science-behind-storytelling.**

  This is a fun podcast on the role of storytelling in science communication, appropriate for how we are framing the hypothesis generation process as a form of storytelling with data and visualization.

- **Xie, Yihui, J. J. Allaire, and Garrett Grolemund (2019).** ***R Markdown: The Definitive Guide.*** **https://bookdown.org/yihui/rmarkdown/. CRC Press.**

- **Xie, Yihui (2019).** ***Bookdown: Authoring Books and Technical Documents with R Markdown.*** **https://bookdown.org/yihui/bookdown/. CRC Press.**

  These are good references when you want to dig deeper into the nuanced options and formats available in RMarkdown.

Class #03: Wednesday 15 September 2021

Cleaning, Transforming, Managing Your Data

One of the most difficult and potenially daunting element of data science is data management. In this class we will introduce data cleaning and transformation tools and strategies for making this task easier. Data cleaning is fundamentally about consistency: we will look at how to systematically identify and correct for inconsistencies and missing data. Data transformation is where we start to manipulate the data to identify trends by filtering to focus on select subsets of your data, sorting, selecting particular variables to focus on, creating new variables from existing variables, and grouping your data. The class concludes with a discussion of how combinations of these basic transforms contribute to hypothesis generation.

Essential Readings

- **Healy, Kieran (2018). *Data Visualization: A Practical Introduction.* 1st edition. https://socviz.co/. Princeton, NJ: Princeton University Press.**

  Read Chapter 1.

  Why are we reading about visualization in the transforms lecture? We want to start thinking about the implications of transforms for how we are going to visualize the data later. It is an iterative process, but having an idea of where one is going saves some (but not all) trial and error.

- **Wickham, Hadley and Garrett Grolemund (2017). *R for Data Science: Import, Tidy, Transform, Visualize, and Model Data.* 1st edition. https://r4ds.had.co.nz/. O'Reilly Media.**

  Read Chapter 10.

  The main rectangular data structure we will be working with most of the semester is called a `tibble`. It is what is more broadly referred to as a `data frame`. As you will see in the readings, when displayed it much looks like a spreadsheet. There is a lot of nuance regarding how you can create `tibbles` and in this Chapter Wickham provides some of the most common.

- **Gastner, Michael T. (2021). *Data Analysis and Visualisation with R.* http://michaelgastner.com/DAVisR2021/.**

  Read Chapter 14 and 15.

  Chapter 14 of Gastner further illustrates illustrates the construction of `tibbles`. Chapter 15 illustrates how to read data into a tibble from `.csv` and `.xls[x]` files.

- **Wickham, Hadley and Garrett Grolemund (2017). *R for Data Science: Import, Tidy, Transform, Visualize, and Model Data.* 1st edition. https://r4ds.had.co.nz/. O'Reilly Media.**

  Read Chapter 5.

Part II: Exploratory Data Analysis

Class #04: Wednesday 22 September 2021

Grammar of Graphics I

Data visualization is part art, part science. This class will introduce you to the grammar of graphics, a modular system of constructing data visualizations. For this class, the objective is to develop an intuition for how different aesthetics are used to highlight trends in your data. It should be stressed this class is intended to develop an intuition of how the grammar of graphics works, we be refining these skills throughout the course.

Essential Readings

- **Healy, Kieran (2018). *Data Visualization: A Practical Introduction.* 1st edition. https://socviz.co/. Princeton, NJ: Princeton University Press.**

  Read Chapter 3.

  You will notice that Healy does not use our friend the pipe function `%>%` as extensively as we do in this chapter. As we learned in the last lecture, the pipe is our friend. That said, Healy illustrates how to make modular, composable visualizations, the foundation of dynamic, automated generation of families of analyses and visualizations. You will develop an intuition about when to modularize and when to use large compositions as illustrated by Wickham as you gain more experience.

- **Wickham, Hadley and Garrett Grolemund (2017). *R for Data Science: Import, Tidy, Transform, Visualize, and Model Data.* 1st edition. https://r4ds.had.co.nz/. O'Reilly Media.**

  *Read Chapter 3, **pay close attention** to the concepts of aesthetics and geoms.*

Optional Readings

- **Wickham, Hadley (2010). "A Layered Grammar of Graphics' '. In: *Journal of Computational and Graphical Statistics* 19.1, pp. 3–28. DOI: 10.1198/jcgs.2009.07098.**

  Many of the concepts laid out in the essential reading are elaborated in technical depth here. It is worth at least a skim

- **Wickham, Hadley (2019). *Ggplot2: Elegant Graphics for Data Analysis.* Third. https://ggplot2-book.org/. Springer.**

  The authoritative reference for `ggplot2` and applying the grammar of graphics.

Class #05: Wednesday 29 September 2021

Grammar of Graphics II

In this lecture we will dig a bit more into the grammar of graphics. Following Healy Chapter 4, we will dive into a few more examples of how aesthetic mappings work, further developing our intuition around the grammar of graphics. Chapter 5 integrates what we have learned about transforms in Lecture 3 with how `ggplot` and the grammar of graphics transform data. In this second half we will focus on how to prepare your analyses for visualization. Finally, we will introduce additional `geoms`, tools for mixing these, and how to better control information about your visualizations in terms of guides and legends.

Essential Readings

- **Healy, Kieran (2018). *Data Visualization: A Practical Introduction.* 1st edition. https://socviz.co/. Princeton, NJ: Princeton University Press.**

  Read Chapters 4 and 5.

Class #06: Wednesday 06 October 2021

Exploratory Data Analysis

In this class we will delve into the art and science of Exploratory Data Analysis (EDA). In this first half of the module will highlight EDA as an iterative, creative process of getting to know your data, in particular the implications of missing values, strategies for filtering and interpolation, and how we use variance in EDA. We will also dig further into how we identify covariance.

Essential Readings

- **Wickham, Hadley and Garrett Grolemund (2017). *R for Data Science: Import, Tidy, Transform, Visualize, and Model Data.* 1st edition. https://r4ds.had.co.nz/. O'Reilly Media.**

  Read Sections 7.1-7.4.

  Review of summary statistics from Wickham, strongly recommended as prep.

- **Wickham, Hadley and Garrett Grolemund (2017). *R for Data Science: Import, Tidy, Transform, Visualize, and Model Data.* 1st edition. https://r4ds.had.co.nz/. O'Reilly Media.**

  Read Sections 7.4-7.8.

- **Bruce, Peter, Andrew Bruce, and Peter Gedeck (2020). *Practical Statistics for Data Scientists, 2nd Edition.* Second. https://learning.oreilly.com/library/view/practical-statistics-for/9781492072935/. O'Reilly Media.**

  Read Chapter 1: Exploratory Data Analysis.

Class #07: Wednesday 13 October 2021

Reading Week

Students will use this week to work on their detailed outlines and exploratory data analyses.

Class #08: Wednesday 20 October 2021

Exploratory Data Analysis II

In this second half of the EDA module we will focus on visualization, in particular aesthetics that help intuitively convey baseline trends, missing values, covariance, and introduce more sophisticated visualizations such as mapping, and how the aesthetics we have used thus far facilitate visualizations of cluster methods we will be using later in the course.

Part III: Visualizing Trends

Class #09: Wednesday 27 October 2021

Mapping

For data with a geographic component, maps are one of the most compeling ways to effectively communicate with your audience. Here, we ask (and answer!): where (geographically or spatially) are we seeing trends and how does it vary across these spaces? In the first part of the class we will use the grammar of graphics to create maps of regions we are interested in, then overlay the results of our EDA(s) onto those maps. In the latter half of the class we will explore how different aesthetics can be used to highlight different facets of our data and analyses, in particular the potential to overlay too much data onto a map, undermining the communication effort.

Essential Readings

- **Healy, Kieran (2018). *Data Visualization: A Practical Introduction.* 1st edition. https://socviz.co/. Princeton, NJ: Princeton University Press.**

  Read Chapter 7.

  We will use the Healy reading to explore a simple form of mapping to *understand the concepts.* The remaining readings illustrate the libraries we will be using in the learning exercises and your projects: the family of packages based on the spatial features package `sf`.

- **Moreno, Mel and Mathieu Basille (2018). *Drawing Beautiful Maps Programmatically with R, Sf and Ggplot2 — Part 1: Basics.* https://www.r-spatial.org/r/2018/10/25/ggplot2-sf.html.**

- **Moreno, Mel and Mathieu Basille (2018). *Drawing Beautiful Maps Programmatically with R, Sf and Ggplot2 — Part 2: Layers.* https://www.r-spatial.org/r/2018/10/25/ggplot2-sf-2.html.**

- **Moreno, Mel and Mathieu Basille (2018). *Drawing Beautiful Maps Programmatically with R, Sf and Ggplot2 — Part 3: Layouts.* https://www.r-spatial.org/r/2018/10/25/ggplot2-sf-3.html.**

Optional Readings

- **Kahle, David and Hadley Wickham (2013). "Ggmap: Spatial Visualization with Ggplot2''. In: *The R Journal* 5.1. https://journal.r-project.org/archive/2013/RJ-2013-014/index.html, pp. 144–161.**

  A bit deeper a dive into `ggmaps` for those interested in mapping for their final project.

- **Lansley, Guy and James Cheshire (2016). *An Introduction to Spatial Data Analysis and Visualisation in R.* London, UK: University College London, p. 121.**

  A bit technical, but worth looking at the later chapters for illustration of spatial autoregressions and inspirations on what to do and what not to do with map visualizations.

Class #10: Wednesday 03 November 2021

Cluster Analysis I

Descriptive statistics are great for looking trends in individual variables and whether *small* subsets of variables move together or not, but we often want to see if we can identify discernable groups, or *clusters*, in a larger dataset comprising many variables. In this class we will learn how to use two of the most common clustering strategies: hierarchical clustering and k-means. In the first half of the class we will visually explore how these clustering strategies work, in effect how they "think about" which observations are similar and which are not. As we will see, sometimes clusters give us compeling, intuitive results; in other cases, they give us gibberish. In the second half of the class we will discuss the role expert qualitative knowledge necessary to interepret cluster analyses and how this contributes to effective, credible hypothesis generation.

Essential Readings

- **James, Gareth, Daniela Witten, Trevor Hastie, and Robert Tibshirani (2017). *An Introduction to Statistical Learning: With Applications in R.* Springer Texts in Statistics 103. New York: Springer.**

  Read Introduction to Chapter 10, Sections 10.1, then 10.3.

  This is the most "mathy" text you will see in the readings; read these introductions to get a feel for how unsupervised learning, in particular clustering, differs from predictive models (regression) many of you are already familiar with. You should read the following items from Imai and Peng, then come back to the remainder of these sections on k-means and heirarchical clustering.

- **Imai, Kosuke (2018). *Quantitative Social Science: An Introduction.* Princeton: Princeton University Press.**

  Read pages 111–115.

  This is one fairly accessible introduction to k-means clustering. After we do a couple of toy clustering examples, we will then explore the congress data Imai uses in this discussion.

- **Peng, Roger D. (2016). *Exploratory Data Analysis with R.* https://bookdown.org/rdpeng/exdata/.**

  Read Section 12 K-means Clustering.

- **Peng, Roger D. (2016). *Exploratory Data Analysis with R.* https://bookdown.org/rdpeng/exdata/.**

  Read Section 11 Heirarchical Clustering.

- **James, Gareth, Daniela Witten, Trevor Hastie, and Robert Tibshirani (2017). *An Introduction to Statistical Learning: With Applications in R.* Springer Texts in Statistics 103. New York: Springer.**

Read Sections 10.3.1–10.3.3.

Read these sections to confirm your understanding from the presentations of the algorithms in Imai and Peng. Do not spend an inordinate amount of time on the math. Pay close attention to the discussion in Section 10.3.3 on validation, interpretation, and clustering strategies.

Class #11: Wednesday 10 November 2021

Cluster Analysis II

We will continue to explore how variables and indvidual observations contribute to clusters. We will then use variants of principal components analysis (PCA), as well as a few other strategies for helping us understand whether the clusters generated by our clustering algorithms are meaningful. We will conclude by illustrating strategies for comparing different sets of clusters as a way to determine which is most effective for the trends and objectives of our analyses.

Essential Readings

– **Kassambara, Alboukadel (2017). *Principal Component Analysis Essentials.* http://www.sthda.com/english/articles/31-principal-component-methods-in-r-practical-guide/112-pca-principal-component-analysis-essentials/.**

Kassambara provides an accessible introduction and tools for principal component analyses. A number of the examples in the lectures are based on Kassambara's examples, so it would be beneficial to work through them before class.

– **Kassambara, Alboukadel (2017). *CA - Correspondence Analysis in R: Essentials - Articles - STHDA.* http://www.sthda.com/english/articles/31-principal-component-methods-in-r-practical-guide/113-ca-correspondence-analysis-in-r-essentials/.**

This reading introduces correspondence analysis, essentially PCA for categorical data.

– **Kassambara, Alboukadel (2017). *FAMD - Factor Analysis of Mixed Data in R: Essentials - Articles - STHDA.* http://www.sthda.com/english/articles/31-principal-component-methods-in-r-practical-guide/115-famd-factor-analysis-of-mixed-data-in-r-essentials/.**

Finally, the FAMD methods described in this reading illustrate how to perform principal component analyses on mixed data sets, those with both quantitative and categorical variables. For many of you doing clustering analysis, this will be the set of tools you will be using.

Optional Readings

– **James, Gareth, Daniela Witten, Trevor Hastie, and Robert Tibshirani (2017). *An Introduction to Statistical Learning: With Applications in R.* Springer Texts in Statistics 103. New York: Springer.**

Skim Section 10.2.

This section of James et. al. provides a bit more of the math behind principal component analyses. It is useful to skim for the intuition, but it is not necessary for the EDA we will be doing in this course.

Class #12: Wednesday 17 November 2021

Text Mining I

Not all data is easily or readly available as quantitative, or even structured, data sets. Identifying trends in groups of text documents (a corpus) is often a powerful complement to traditional qualitative analysis. In this class we will introduce the principles of text mining, its strengths and limits, and the fundamentals of transforming a document into data structures we can use to identify trends. Next we will explore a rather intuitive form of text mining: sentiment analysis. Finally, we will begin our first discussion on the strengths, weaknesses, and potential pitfalls in text mining, how how to navigate these in the process of hypothesis generation.

Essential Readings

- **Silge, Julia and David Robinson (2017). *Text Mining with R: A Tidy Approach.* 1st edition. https://www.tidytextmining.com/. O'Reilly Media.**

  Read Chapters 1 and 2.

Class #13: Wednesday 24 November 2021

Thanksgiving

Go eat turkey. Tell your family how much you love data science :)

Class #14: Wednesday 01 December 2021

Text Mining II

In this lecture we will continue our exploration of text mining by working through two common analyses: frequency analysis and relationships amongst groups of words. We will also see yet another instance of integrating analyses, representing relationships between words as networks. In the second half of the lecture we will continue our focus on visualization and how this contributes to hypothesis generation.

Essential Readings

- **Silge, Julia and David Robinson (2017). *Text Mining with R: A Tidy Approach.* 1st edition. https://www.tidytextmining.com/. O'Reilly Media.**

  Read Chapters 3 and 4.

Class #15: Wednesday 08 December 2021

Project Presentations

In this class students will present their final projects.

Assignments and Writing Guidelines

The following provides details on the assignments for the course. All written assignments *must be submitted in PDF format* and conform to the writing format guidelines. Policy research project milestones and learning exercises will be submitted via GitHub. **All assignments are due *at or before 2359* on the assignment due date.**

Assignments

The best way to learn data science is by doing. In addition to the policy research project, you will also have 5 learning exercises.

As a note on writing requirements, the length requirements for assignments and project milestones are described in terms of *maximum* word count. For the page equivalent, 500 words is *approximately* 1 page with 1 inch margins, **single-spaced**, 12 pt Times New Roman (or a very similar serifed font like the one used in this document).

Participation

You will start with 7 (out of a possible 10) points. You are expected to have completed all of the readings for a given week before the class and be ready to discuss those readings in class. Portions of each class will be run seminar style, with the expectation that students discuss the concepts and issues at hand in a civil, constructive, yet rigorously analytic manner. This is your opportunity to gain points. If you attempt to participate and clearly demonstrate you have not done the related reading, you will definitely lose participation points. That said, informed, thoughtful, civil, and constructive disagreement with other students or Dr. Sowell is encouraged, especially when Dr. Sowell makes intentionally leading, biased, or contradictory assertions to encourage discussion and creativity.

Also, as a note on participation, we will be using laptops extensively for exercises in the course. Beyond this, Dr. Sowell encourages students to *quickly* look up relevant materials online to contribute during discussion. That said, refrain from spending class time on e-mail, social media, instant messaging, or anything else that is not directly related to the class or discussion at hand.

Learning Exercises

The learning exercises are intended to be short sets of exercises to further familiarize yourself with topics from class. These will be distributed via the course GitHub repository. They will be submitted by pushing the completed files to your personal GitHub repository for the course. We will set up personal repositories during the second class meeting on Wednesday 08 September 2021.

Policy Research Project

The objective of the policy research project is for you to apply lessons and concepts learned in the course to a policy or governance issue area *of your choice*. For the policy research project you will identify a data set (or sets) that you would like to explore, visualize, and evaluate.

Your first task is to Identify a data set of interest to you, that you believe you can do an in-depth analysis of for your policy research project. Your proposal should demonstrate you are generally familiar with the data and you have done some basic analysis. Dr. Sowell will have to approve this data set. You should select your data set early and set up a time to discuss the data set with Dr. Sowell **well before** the proposal deadline to get preliminary approval.

There is no minimum word limit on the policy research research project. The maximum word limit is 10,000 words, approximately 20 pages, not including figures or references. See the writing guidelines for specifics on what does and does not contribute to the word count.

Students are *required* to maintain the references used in their assignments, in particular for the policy research project, in Zotero. If the student has not already, the student should create a Zotero account.

Policy research project milestones:

1. **Zotero Policy Research Project Group:** due *Friday 03 September 2021*

   Deliverables:

   – e-mail to Dr. Sowell (jsowell@tamu.edu) confirming the student has
     1. installed and setup Zotero
     2. joined the Zotero group for this course
     3. created their own group for this course

   Students will use Zotero to create a shared group (library) entitled `Z - DS - lastname` (formatted exactly as here, with the spaces, where `lastname` is your last name) and use Zotero's group invitation function to invite Dr. Sowell (jsowell@tamu.edu) to the group. The Zotero Group should be private and Dr. Sowell should have edit rights so he can share references with the student. **This task is worth 3 points of your final grade. If you do not set up and share your Zotero library by 2359 on you will lose these points permanently.** For step-by-step instructions on setting up

Zotero, see the section on Zotero Configuration in the Appendix. If you have any questions or run into any problems, please e-mail Dr. Sowell (jsowell@tamu.edu) at least one hour before class on .

All references used in the policy research project *must* be saved in the student's shared Zotero library. This will make your life a lot easier: you can easily copy references from the course library to your library for use in your policy research project, it allows Dr. Sowell to review your policy research project references with you, and allows Dr. Sowell to share relevant references with you when appropriate. When adding references to journal articles, reports, etc., you should make sure the PDF of the document is attached to that entry. The Zotero Connector will often do this for you, but you should double check and add the PDF if it does not.

Students will maintain data and R project files for milestone deliverables in their GitHub repository. We will setup the GitHub repositories in the second class meeting on Wednesday 08 September 2021.

2. **Proposal:** *(5%)* due *Monday 20 September 2021*

   Deliverables:

   - **`.Rmd` file** of the proposal document (in the `templates` directory of your final project repository), with proper references and citations to the dataset to be used
   - **PDF** of the proposal document
   - data should be in the `data` folder of your project repository
   - `.Rmd` document (in the `templates` directory of you final project repository) illustrating baseline data import and simple summary statistics of your dataset(s), including variables of interest, their types (number, categorical, text), and a brief description of each variable.

   The proposal should be a 500 word (max) description of the policy or governance issue you plan to address with the dataset(s) you have selected for your policy research project.

   At a minimum, the proposal document should reference readings from the course (with a bibliography that does not count against the 500 word limit). A *good* proposal will also include references to materials outside the course that (1) support the analysis strategies and arguments in the proposal and (2) demonstrates the student has already started their own research on the topic.

   In terms of the structure of the proposal, it should answer the following questions:

   1. What is the issue you are addressing?
   2. Why is this issue important?
   3. What data are you using to explore this issue?
   4. What has already been done with this data?
   5. What questions are you trying to answer? Relate your questions to what has already been done, this will require some amount of literature review relative to your dataset.
   6. Why is what you are doing different from other analyses and visualizations you have found? How does this data exploration contribute to answering your questions (again relative to other work)?

3. **Detailed Outline and EDA:** *(20%)*, due *Monday 15 November 2021*

   Deliverables:

   - .Rmd file of the detailed outline document with the EDA appendix
   - PDF of the detailed outline

   The objective of the detailed outline is to articulate the fundamental structure of the project report, the current status of analyses and arguments, supporting materials, and how these are used to support the analysis and argument. The outline is intended to get the student thinking about the structure of the argument; it is expected to change based on feedback and further analysis leading up to the rough draft. That said, the detailed outline should articulate a clear and coherent narrative, argument, and supporting analysis.

   You should copy the template for the final policy research project in the `templates` directory of your project GitHub repository as the template for your detailed outline. The outline portion should flesh out the sections of the body of the policy research project following the guidelines below. The detailed instructions for the EDA, which should be in the appendix of your detailed outline, is in the EDA section (in the appendix) of the policy research project template file.

The outline (the body of the document) should comprise

- a title (title, name, date, no abstract at this point)
- the approved proposal, followed by
- the outline with enumerated headers (1, 2.3, 5.6.3, etc.) for the major sections, subsections, etc.
- enumerated sections should include an "opener" and a "closer" that conveys the content for that section:
  - the overall objective of the detailed outline is to tell the high-level story of the argument and analysis
  - the "opener" (1-3 sentences) is like an opening paragraph: it introduces the topic, problem, argument, or analysis to be presented in that section
  - the "closer" (1-3 sentences) is like the concluding paragraph: it articulates the take-aways of a narrative, summary of the problem, highlights of the argument, or conclusions of an analysis
  - sentences in both the opener and closer should be substantive declaratives, **not** "This section will do this" or "This section will show that"
- the exploratory data analysis (EDA, the appendix) is an opportunity for you to demonstrate you have systematically explored your data set; the details of the EDA specification can be found in the appendix of the policy research project template document in your GitHub repository

4. **In Class Project Presentation:** *(5%)*, due *Tuesday 07 December 2021*

   Deliverables:

   - PDF of the presentation slides

   On the last day of class students will present their policy research projects. Each student presentation will be approximately 20 minutes followed by discussion. Slides are required for the presentation. Slides should uploaded to the `Project Presentation` collection in the student's Zotero library at least two hours before class on .

5. **Policy Research Project Report:**, *(30%)* due the last day of exam week *Wednesday 08 December 2021*

   Deliverables:

   - .Rmd of the final policy research project report
   - PDF of the final policy research project report

   Final policy research project reports will follow the same format as the rough draft. The final project report should incorporate changes, suggestions, and comments made on the rough draft. Dr. Sowell will compare the rough draft and final draft when grading the final report.

Write-Up Formatting Guidelines

The following describes Dr. Sowell's standard writing guidelines. That said, we will be using an R Markdown template for all of our assignments and your policy research project. While these requirements may *seem* daunting, the RMarkdown template will take care of most of them. Following the ethos of Markdown and the reproducible research paradigm, the objective is to get the formatting out of the way so the analyst can focus on writing and analysis.

These guidelines are not optional and will be strictly enforced. If you submit material that does not conform to these guidelines, it will be returned ungraded and with a 10% late penalty.

- single-spaced
- title page with title, name of author, and abstract; title page should not have a page number

- title page and abstract (approximately 300 words) do not contribute to word count for assignment unless otherwise specified
- font should be New Times Roman or similar serifed font
- font size for abstract and body of text should be 12 pt
- document should be fully justified as in books and journal articles, no ragged right edge
- use enumerated footnotes, 10 pt; *do not ever use endnotes*
- 1 inch margins all around (left, right, top, bottom, this is standard in Word)
- block quotes consistently inset from left and right margins
- page enumeration in footer, no page number on title page, body enumeration starts starts at page 2
- enumerate sections and subsections (1, 2.1, 3.5.2, etc.)
- figures should be labeled ("Figure 1: Scatter plot of data set X", "Figure 2: Distribution of variables in category Y", etc.), referenced by figure number ("Note that the distribution in Figure 4 is left skewed. . . "); figure labels will contribute to word count
- references must be stored in Zotero
- inline references and bibliography should follow Chicago author-date format
- the bibliography will not contribute to the word count
- inline references:
  - materials (articles, books, etc.) with page numbers must include the page number or page range that includes the quote or evidence referenced
  - materials, such as web pages that are not enumerated, should include the finest grained subsection containing the quote or evidence where the page number or page range would be in the inline reference
  - inline references that do not follow these guidelines will result in assignment returned with a 10% penalty
- documents submitted should be in PDF format and should allow highlighting of text using PDF annotation tools such as Adobe Acrobat Reader; you should check this as you write and before submitting, exotic invisible formatting in Word occasionally breaks this requirement
- PDF documents will be submitted electronically either via Zotero or via e-mail to jsowell@tamu.edu depending on the assignment guidelines; hard copy will not be accepted

Dr. Sowell will provide an example PDF to illustrate these guidelines. When grading your assignments, Dr. Sowell will annotate your document electronically. Any mainstream PDF reader, such as Adobe Acrobat Reader, Skim, or Apple's Preview will render these comments. A comment attached to the title of the assignment will contain the total grade and overall comments. Graded essays and write-ups will be returned to you electronically.

University Policies

Attendance

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Other absences may be excused at the discretion of the instructor with prior notification and proper documentation. In cases where prior notification is not feasible (e.g., accident or emergency) the student must provide notification by the end of the second working day after the absence, including an explanation of why notice could not be sent prior to the class.

On some occasions, the instructor may have to miss a class due to administrative or academic responsibilities out of town. If it does occur, the instructor reserves the right to reschedule class at a time when the vast majority of students are available for the make-up class and will convey the material to students unable to attend the make-up during office hours.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student's grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

"Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor" (Student Rule 7, Section 7.4.1).

"The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence" (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code (see Student Rule 24).

Academic Integrity Statement and Policy

"An Aggie does not lie, cheat or steal or tolerate those who do."

"Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one's work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case" (Section 20.1.2.3, Student Rule 20).

You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

Dr. Sowell strongly encourages reading groups for discussing course materials, but not for distributing the reading load. Dr. Sowell also recognizes the role and efficacy of group learning and peer review of assignment deliverables, such as proof-reading one another's work and/or discussing the structure and flow of arguments presented in assignments. If you engage in this kind of collaboration, you must add a footnote to the your name (as the author) with a statement indicating who you collaborated with and how they contributed to the work you are turning in under your name. As an example, "John Smith proof-read a draft of this assignment, providing editorial comments and suggesting I rearrange the order of my cases to improve the logical flow of my case studies section." Another example would be "I discussed this assignment with Jane Smith and she suggested the articles (Warner 2016; Billings 1967), which I have included in this work."

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact Disability Resources in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu. Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

Title IX and Statements on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see University Rule 08.01.01.M1):

- The incident is reasonably believed to be discrimination or harassment.
- The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written class assignment or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, you will be able to control how the report is handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with Counseling and Psychological Services (CAPS).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in proper self-care by utilizing the resources and services available from Counseling & Psychological Services (CAPS). Students who need someone to talk to can call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Appendix

Zotero Configuration

The following instructions describe how to set up the Zotero App and create a shared group library.

Zotero App Setup

1. Create a Zotero account at https://www.zotero.org using your `@tamu.edu` e-mail address.

2. Install

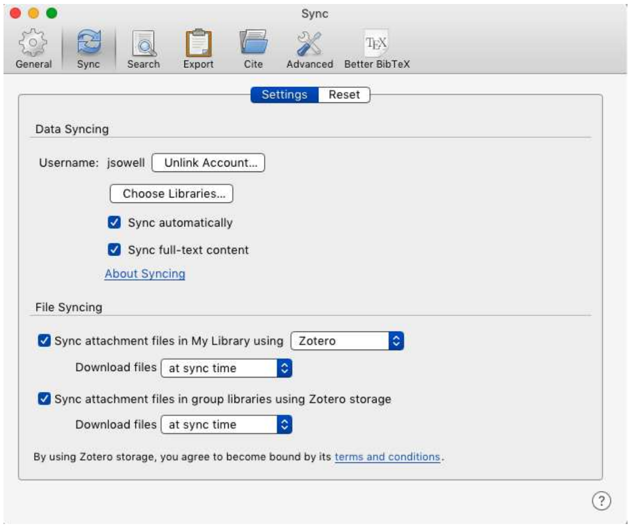
    1. Zotero app, available at https://www.zotero.org/download/
    2. Install the Zotero Connector web browser plugin, available at https://www.zotero.org/download/connectors

3. You should receive an invitation to the course library in both the e-mail you set up your account with and in the Zotero Inbox, available via the Zotero web interface.

4. To confirm your Zotero app is syncing with the course library, you should check your Zotero app preferences. In the `Preferences` window, select the `Sync` tab and confirm that

    - Zotero shows `Username: your_username` (where `your_username` is your username)
    - you have checked `Sync Automatically` and `Sync full-text content`
    - you have checked `Sync attachment files in My Library using Zotero` and selected `Download files at sync time`
    - you have checked `Sync attachment files in gorup libraries using Zotero storage` and selected `Download files at sync time`

    A screenshot illustrating what your settings should look like can be found below.



Data Syncing

Username: jsowell

☑ Sync automatically

☑ Sync full-text content

File Syncing

☑ Sync attachment files in My Library using Zotero

Download files at sync time

☑ Sync attachment files in group libraries using Zotero storage

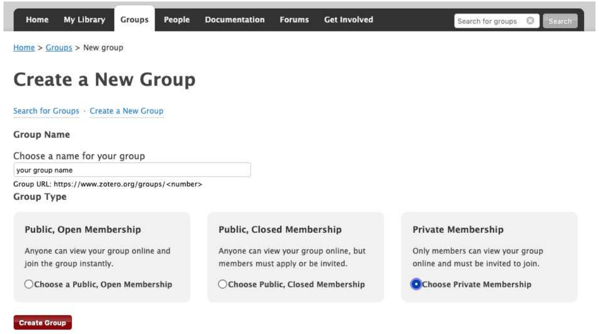
Download files at sync time

By using Zotero storage, you agree to become bound by its terms and conditions.

If you prefer not to sync automatically, uncheck `Sync automatically`. ***If you choose this option you will have to explicitly sync your libraries using the small circular green arrow in the upper right of the Zotero app.***

Shared Groups (Library) Setup

1. Log in to the Zotero web interface at https://www.zotero.org
2. Click on the `Groups` link
3. Click `Create a New Group` link directly under the header `Zotero Groups`
4. Add a name for your shared library where it says `Choose a name for your group` and select the `Group Type` as `Private Membership` as illustrated below



Create a New Group

Group Name

Choose a name for your group

your group name

Group URL: https://www.zotero.org/groups/<number>

Group Type

Public, Open Membership

Anyone can view your group online and join the group instantly.

○ Choose a Public, Open Membership

Public, Closed Membership

Anyone can view your group online, but members must apply or be invited.

○ Choose Public, Closed Membership

Private Membership

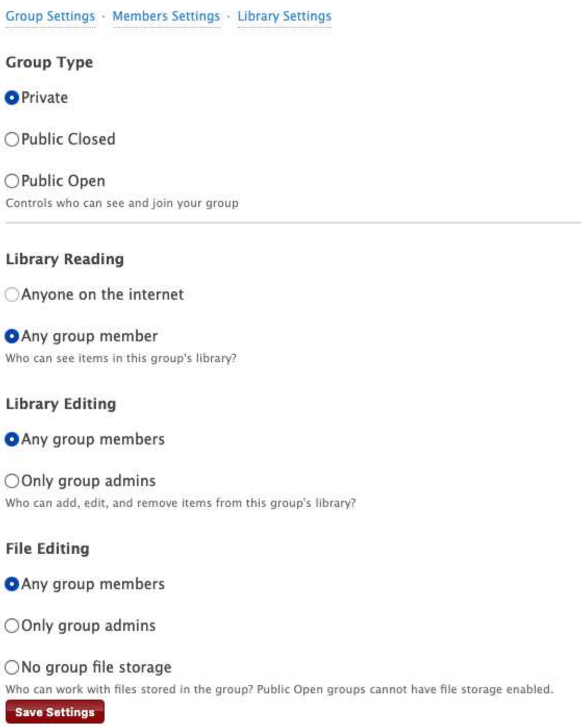
Only members can view your group online and must be invited to join.

● Choose Private Membership

5. Click the `Create Group` button
6. Select the following group settings (illustrated in the screenshot below):

   - for `Group Type`, select `Private`
   - for `Library Reading`, select `Any group member`
   - for `Library Editing`, select `Any group members`
   - for `File Editing`, select `Any gorup members`

   then click `Save Settings`; these are the defaults, so you should not have to change anything.



Group Type

● Private

○ Public Closed

○ Public Open

Controls who can see and join your group

Library Reading

○ Anyone on the internet

● Any group member

Who can see items in this group's library?

Library Editing

● Any group members

○ Only group admins

Who can add, edit, and remove items from this group's library?

File Editing

● Any group members

○ Only group admins

○ No group file storage

Who can work with files stored in the group? Public Open groups cannot have file storage enabled.

7. To add new members to the group, click the blue link `Member Settings` link under the heading `groupname: Member Settings` and click the link `Send More Invitations` at the bottom of the page and follow the instructions there.

Notes on Zotero Connector Plugin

The Zotero Connector adds a small icon to the right of the address bar in your web browser (upper right corner of the window). To use the Connector, the Zotero app must be open. By default, when you click the Zotero icon to download a given reference, it will automatically put that reference *in whichever folder you currently have selected in the Zotero app.* This is quite convenient if you have organized your research folder into topic specific subfolders, or, in my case, if you have it organized by class and category of reading material (essential, optional, etc.).