2201 Crescent Pointe Parkway, Apt. 4302
College Station, TX 77845
m: +1 517 214 1900
e: jesse.sowell@gmail.com

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 the Department of Science, Technology, Engineering, and Public Policy 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. I hold an interdisciplinary PhD in Technology, Management, and Policy from MIT's Engineering Systems Division, integrating computer science, international political economy, and operations strategy. My research focuses on the political economy of Internet infrastructure and security, in particular the norms and best practices of private transnational cybersecurity regimes and how these actors engage with state-based security organizations and law enforcement. Empirically, my work builds on extensive engagement with global expert practitioner communities that ensure the security and stability of the Internet's infrastructure and online platforms. I not only thrive in multidisciplinary environments—I consider them my native habitat. My intrinsically interdisciplinary background would be a rare and valuable complement to the research, teaching, and impact of the Department of Science, Technology, Engineering, and Public Policy—I am especially excited at the opportunity to contribute to the work of the Digital Technology Policy Lab.

My applied research is driven by real-world problems in today's digital platforms—real-time management of emerging cybersecurity threats; digital platform governance and its implications for markets and innovation; the governance of connectivity platforms in developed and developing regions; and the role of industry in mitigating disinformation campaigns. These kinds of 'wicked issues' cannot be resolved by policy formulation and implementation by a single stakeholder group or jurisdiction. Addressing these issues requires combining technical, operational, organizational, and legal capabilities distributed among equally diverse sets of state and non-state, private actors. The research and policy challenge central to my work is understanding how to systematically harness the capabilities and capacities of the diverse actors that sustain the security, stability, and integrity of complex infrastructures such as the Internet to solve global policy problems.

My work addresses two key parts of this challenge. First, my empirical work builds on established theories of institutional design and political economy to understand how transnational epistemic communities develop, and adapt, the norms, standards, and best practices they use to cope with uncertainties endemic in complex engineering systems such as the Internet and digital platforms. Second, I evaluate the feedback loops necessary to systematically integrate this knowledge into the policy-making processes of international organizations and governance structures, while being cognizant of the politics of science and technology policy advice. I believe my work identifying and closing these knowledge gaps, building bridges between the communities that manage the Internet and policymakers, is exceptionally aligned with STEAPP's mission and I am excited for the opportunity to contribute to the research and policy agenda of the Digital Technology Policy Lab.

Research

My research strategy has always been interdisciplinary. I started my academic life in computer

science as a software engineer, focusing on programming languages 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 in Internet infrastructure management and cybersecurity. I funded the last year of my dissertation work as the primary author on a Google Faculty Research Award ($85,000).

As a Postdoctoral Cybersecurity Fellow at Stanford, I was the primary author on two grants (totaling $125,000) evaluating the thus far ad hoc collaboration between global threat cybersecurity and threat intelligence communities and law enforcement. At Stanford, I developed and managed the research plan, milestones, and budgets; regularly reported findings and progress to funders and collaborators; managed research assistants contributing to data collection and literature reviews; and planned and executed workshops and focus groups (colocated with cybersecurity and Internet operations conferences) comprising cybersecurity professionals, law enforcement, lawyers, and policymakers in the US, Africa, and Europe. In my cumulative report, I evaluated these ad hoc relationships in terms of credibility and legitimacy norms within closed, often hidden, private intelligence groups; across collaborative relationships between these actors and law enforcement; and the challenges to developing credibility and legitimacy in domestic and international law enforcement and governance regimes. More recently, in collaboration with colleagues at the Shadowserver Foundation, we are continuing this work in a report for Europol detailing from technical, legal, and international collaboration challenges faced in the recent Avalanche takedown, representing the largest concerted application of mutual legal assistance treaties (MLATs).

A central focus of my work is the consensus-based coproduction of these institutions' expert knowledge, how it sustains the capabilities and capacities necessary to adapt to the uncertainties endemic in evolving digital platforms, and the challenges of integrating this knowledge into global and domestic policy development, regulatory design, and governance processes. In my chapter on planned adaptation, I evaluate successful instances of systematically integrating epistemic communities' knowledge of complex engineering systems into regulation and policy. In collaboration with Dr. I. Brass, our article in Regulation & Governance argues for a novel, planned adaptive regulatory framework that closes the feedback loops between IoT security regulations and standards development and the expert knowledge of epistemic communities necessary to keep pace with innovations by cybercriminals taking advantage of low-margin, insecure IoT devices. My article in the Journal of Cyber Policy comparatively evaluates the governance of digital platforms, contrasting the roles of control and consensus-based knowledge coproduction for monitoring predatory practices, highlighting the need for coregulatory models that integrate accountability mechanisms with monitoring capabilities to ensure fair and equitable digital marketplaces. My recent submission to International Organization offers an empirical deep dive into the understudied institutions in the Internet's routing system, contributing to the literature on epistemic communities by explaining how these institutions function as epistemic authorities and offering a framework for evaluating how to more effectively integrate these into the broader global governance system. Across each of these studies, the common theme is the collaborative application of consensus-based, coproduction of knowledge and regulatory authority to solve wicked global policy problems.

I also lead the Internet Infrastructure and Policy Lab (IIPL), coordinating the work of four student researchers. IIPL projects have a distinct focus on development dynamics in developing regions. Their projects include:

1. the politics and governance of submarine cables critical to modern Internet communications

(a publication in the Journal of Public and International Affairs on submarine cables and the South China Sea conflict; an article under review by Contemporary Security Policy characterizing submarine cable governance challenges for regional economic and security across six cases);

2. studies on how autocracies are using Internet shutdowns (a five-case study developing a conceptual model of the relationships between kinds of autocratic regimes and their use of Internet shutdowns in Africa, under review by Journal of Peace Research; current work is operationalizing this model, applying cluster analysis to a global dataset from Access Now on Internet shutdowns from 2016 to 2021)
3. an evaluation of the role of Internet infrastructure development in developing regions, with a special focus on Africa and Latin America;
4. a multilevel network analysis (combining organizational and individual ties) among the globally diverse institutions that ensure stability, safety, and security of the Internet

While each researcher has their own projects, work in the IIPL is a distinctly collaborative endeavor, convening weekly to share progress and discuss current challenges, celebrate significant milestones, and share and exchange domain and methods expertise.

Engagement and Impact

Stakeholder engagement is essential to my empirical and theoretical work. Over the last ten years I have interviewed over 100 actors across network operator communities, digital platform managers, and cybersecurity and hacking communities, at over 40 network operations and cybersecurity conferences around the world. I have invested significant time and effort in developing rapport with these understudied and hidden communities. I am also distinctly cognizant of balancing my research obligations and my ethical obligations to research subjects, many of whom face regular threats from transnational cybercrime organizations. By demonstrating I speak technical, political, 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 and more conventional government and law enforcement agencies. Since the beginning of my fieldwork in 2012, I have developed and sustain 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 theory-based understandings of the kinds of collaboration necessary for keeping pace with continuous innovation by cybercriminals.

I am proud to say that my recent work integrates fieldwork and engagement with regional and global collaborators to create real-world impact. Recent engagements have focused on (1) understanding how these transnational regimes engage in systematic, sustainable information sharing with state actors and (2) developing strategies for promulgating cybersecurity norms and best practices. This work has created impact on both sides, and is essential to collecting the empirical data necessary to understand the coproduction of knowledge necessary for effective regulation and policy for managing complex, transnational infrastructures such as the Internet. As a research fellow and advisor to the Anti-Phishing Working Group (APWG), I was the program chair of 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; we are now planning annual Cybersecurity Data and Governance

symposia, starting in November 2022. My ongoing work with the APWG (in collaboration with Dr. L. Weissinger at Tufts' Fletcher School of Global Affairs) is evaluating the perverse incentives created by ICANN's ill-conceived GDPR compliance and working with Senator Ed Markey's (D, MA) staff to develop model legislation that ensures the availability of data critical to cybersecurity incident response.

As a senior advisor to the Messaging, Malware, and Mobile Anti-Abuse Working Group (M^3AAWG), starting in 2016 I worked with the M^3AAWG 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^3AAWG's IoT Special Interest Group (SIG), working with Internet Service Providers (ISPs) to understand and evaluate the feasibiliy of IoT reputation models. I have included reference letters detailing these engagements from APWG and M^3AAWG leadership in the supporting documents.

Developing these global partnerships has given me substantial access to technical, law enforcement, intelligence, and international organizations actively navigating processes for more effectively collaborating to combat cybercrime. Through these applications of my research on collaboration and governance I have created regional and global impact, helping to create organizations that continue to develop cybersecurity capabilities and capacities, in collaboration with global partners in the cybersecurity, law enformcement, and policy communities. It also provides unique insight into the real-world challenges of developing these collaborations, valuable as pragmatic empirical evidence for both theory- and policy-relevant research. Many of these organizations have substantive demand for engagement with scholars that can help them better leverage their knowledge and capabilities in the international system and global governance. This access and experience, not only understanding the technical, governance, and engagement challenges, but also understanding the diverse cultural and regional challenges, also contributes to my research-led teaching.

Teaching

Understanding the social, political, and economic challenges presented by emerging trends in Internet operations, operational cybersecurity, online platforms, and cybercrime requires engaging students in contemporary, real-world problems. In my current role I developed my department's Cyber Policy Concentration[1] from the ground up, creating a comprehensive curriculum and development programme for masters students in both the Department of International Affairs and the Department of Public Service and Administration. This interdisciplinary, research-led programme (now in its third year) provides accessible deep dives into digital technologies that highlight the politics of these complex systems' design, operations, and security.

The four courses I developed and teach in this program have been well received by students and faculty:

- *Introduction to Cyber Policy* offers foundations in policy and governance issues related to Internet infrastructure management, jurisdiction and attribution challenges, privacy and surveillance, encryption, consolidation, disinformation, and cybercrime, among others.
- *Data Science and Visualization for Policy Analysis* focuses on applying exploratory data analysis methods, such as cluster analysis and visualization, for hypothesis generation and case selection. Although based on R, I have specifically designed this course for students with

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

little to no programming experience; it can be scaled down for undergraduates or up into doctoral level course. I have included the flier and syllabus for this course in the attached supporting documents.

- *Internet Infrastructure: Platforms and Politics* focuses on the governance and politics of online platforms and infrastructures that intermediate our social, political, and economic lives (such as Facebook, Google, and mobile platforms). This is an advanced course for students interested in a deeper dive into topics such as the politics and transnational security challenges facing specific elements of the infrastructure such as submarine cables, Internet routing, and the nuanced intersection of platform economics and security.
- *Advanced Cyber Policy* takes a deep dive into the diverse complex of institutions shaping Internet governance, political authority and legitimacy challenges facing these institutions in the broader global governance system, and co-regulatory approaches to effectively developing cyber policy.

I have also led group projects and cumulative capstones in which students engage with public and private stakeholders to apply these lessons first-hand. Building on my research, I have led capstones engaging with the National Cyber Forensics Training Alliance (NCFTA) and the FBI to understand the challenges of collaboration between private cybersecurity actors and international law enforcement, with a focus on business e-mail compromise, ransomware, and synthetic identity scams.

I have considerable experience teaching, developing, and evaluating technology and policy programmes, focusing on a pedagogy that integrates understanding the technical (complex system) dynamics necessary for rigorous, evidence-based technology policy analysis and prescriptions. This balance prepares students to be not only effective analysts and scholars at the policy-level, but to also serve as the increasingly important bridge between technologists and state actors on topics such as privacy and surveillance, cybersecurity, disinformation and misinformation, platform politics, and transnational infrastructure management. This fundamentally interdisciplinary education in technology policy is in increasingly high demand by students, academia, and public and private sector employers—I cannot count the number of times colleagues in both the public and private sector have asked me to send them good students that understand the nuance of the technologies at play, *and* domestic and international policy processes. I am extremely excited at the potential opportunity to further develop both the applied and theoretical elements of this curriculum with colleagues in STEAPP and the DTPL. I also welcome the opportunity to adapt my curriculum to complement existing undergraduate, masters, and doctoral curricula. In particular, I believe my interdisciplinary background in engineering systems, political economy, and cybersecurity could substantively contribute to the Centre for Doctoral Training in Cybersecurity.

I am quite excited at the prospect of bringing my ongoing research projects, teaching, access to expert networks, and engagement initiatives to 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