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 (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 work focuses on the political economy of Internet infrastructure and security, building on extensive fieldwork to explain and evaluate how epistemic communities create and sustain the knowledge and rules necessary to keep pace with technological change, demands for diverse online services, and emerging threats. Integrated 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. The insights from my research on the understudied epistemic communities are essential to systematically and effectively integrating these untapped resources 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. In the last four years my teaching has integrated this work into a comprehensive, research-led cyber policy programme, blending theory, case studies, and innovative teaching methods to *(1)* develop students' critical thinking skills *(2)* applied to project-based deep dives into substantive domains that *(3)* that hones the skills necessary for policy analysts and researchers to bridge the gaps between policy and technical communities.

My current and emerging research, ongoing policy engagement, and well-developed cyber policy curriculum is exceptionally well-suited to STEaPP and the Digital Technologies Policy Lab (DTPL). My ongoing and recently developed projects complement existing work in STEaPP's infrastructure and development research clusters. My new projects on co-regulatory approaches to combating disinformation and data governance would be a substantive contribution to the DTPL's portfolio. I explicitly designed my department's cyber policy curriculum, from scratch, explicitly for social scientists from diverse intellectual backgrounds. My introduction to cyber policy and data science courses can easily be adapted for an undergraduate curriculum; based on the feedback from four years of guest lectures at STEaPP, I know advanced courses will appeal to students in the digital route, STEaPP doctoral students, and students in the Cybersecurity Doctoral Training Program. The DTPL and the Policy Impact Unit would ideal homes for my ongoing engagement programmes with industry and non-profit partners on cybersecurity data governance and the ongoing challenges facing collaborations between technical communities and law enforcement. I believe my intrinsically interdisciplinary portfolio is a rare and valuable complement to STEaPP's mission and programmes, and that STEaPP is where I can make the most impact, enhancing my research through collaboration with others, and continuing innovate in my teaching and engagement programmes.

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 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. The cumulative *Combined Capabilities* report evaluated these collaborations in terms of credibility and legitimacy norms within these groups and in the broader global governance system. 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 from the Avalanche botnet takedown, one of the largest concerted applications of Mutual Legal Assistance Treaties to date.

My research has three common themes: *(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 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, travel funded by the Internet Society) 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), I make empirical and theory contributions to the Internet governance and epistemic communities literature. Empirically, I explain how institutions coordinating the Internet's infrastructure, in the absence of state regulation, developed the rules and accrued epistemic authority. My characterization of epistemic authority is a novel theoretical contribution, and I use it to offer prescriptions on how to more effectively integrate these authorities into the broader global governance system. I believe my common research themes 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 created the Internet Infrastructure and Policy Research Group (IIPRG), where I supervise four masters-level student researchers. 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 shutdown global data from 2016 to 2021. These research streams would not only enhance the DTPL's portfolio with novel and impactful research, but also creates fruitful linkages with the 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, and across STEaPP on these kinds of projects.

Engagement and Impact Through Science Diplomacy

My deep, novel 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 diplomacy. 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, policy makers and 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 rich, theory-based 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 with the APWG (in collaboration with Dr. L. Weissinger at Tufts' Fletcher School of Global Affairs) we evaluate 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.

As a senior advisor to the Messaging, Malware, and Mobile Anti-Abuse Working Group (M^{3}AAWG), starting in 2016 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 the development of impactful organizations that continue to develop cybersecurity capabilities and capacities in developed and developing regions. This engagement provides unique insights critical to my work. 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 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. 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.*

In my current role I designed, developed, and deliver, from scratch, my department's Cyber Policy Concentration (CPC),[1] offering a comprehensive curriculum and development programme for masters students coming from diverse disciplinary backgrounds. This interdisciplinary, research-led programme (now in its third year) provides accessible deep dives into digital technologies and the politics of these complex systems' design, operations, and security. I developed 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 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 & Regulation and Digital (need the full name). I am familiar with STEaPP's curriculum and course structure, and would love to work with STEaPP colleagues to integrate my courses into the

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

Digital route's educational experience and identify cross-over topics with other routes. The first two above can be easily scaled to advanced undergraduate courses (syllabi included in supporting documents); the latter are appropriate for advanced MPA students and can be adapted for doctoral students. I am also keen to contribute to STEaPP's cumulative group projects. In addition to relationships with law enforcement, I have extensive relationships with organizations such as the Cyber Defense Alliance (CDA, based in London) and the Global Cyber Alliance (GCA, offices in London) that would be excellent partners for MPA group projects in the Digital Route. I also have substantive experience with the broader dynamics of technology and policy programmes: I have recently joined the advisory board for the Program on Emerging Technologies (PoET) hosted by MIT's Political Science Department, I have participated in and helped coordinate the Technology, Management, and Policy Consortium for graduate research into technology and policy, and, through these experiences, I have learned about the diverse approaches to technology and policy education through engagement with STEaPP's sibling programmes such as Engineering and Public Policy (EPP) at Carnegie Melon University and the Department of Technology, Policy and Management at TU Delft.

I am extremely 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