DATA&
SOCIETY

## Researcher/Postdoctoral Scholar, Socio-technical Security

Job Posting
October 2019

Data & Society Research Institute is seeking an engaging and collaborative Researcher/Postdoctoral Scholar, Socio-technical Security to join our growing Research team!

**About the Socio-technical Security Project**
Social media, search engines, mobile phones, and other internet-based services have reconfigured how people access information and communicate with others around the globe. These technologies have also introduced new social and cultural vulnerabilities, and modulated old ones. Conspiracy theories and misinformation quickly proliferate across networks. Trust in institutions, experts, and information intermediaries is declining for a variety of reasons. And adversaries with economic, political, and ideological incentives are helping manufacture ignorance.

The field of computer security matured under similar conditions, as computers were first exposed to networking environments--drastically increasing their attack surface. As computer hackers set out to demonstrate this new insecurity, in both friendly and malicious ways, a complex field of security research consisting of formal and informal researchers, public and private institutions, contentious norms and standards, and a range of market dynamics emerged to grapple with the new threats. Focusing primarily on how attackers exploit technical vulnerabilities to gain or deny access to systems, the bulk of this work continues to emphasize technical controls. Nevertheless, a growing class of manipulators now use systems as they are technically designed to function--even if they use them counter to the spirit their designers intended or imagined could be possible; they exploit features, rather than bugs, in pursuit of social and cultural outcomes that often contravene the policies of platforms, frustrate the efforts of moderation teams, and threaten the healthy functioning of communities.

This initiative puts the socio-technical--the interplay between social and technical systems--at the center of analysis, recognizing that the information and communication landscape involves complex interactions between social norms and technical systems. As such, the vulnerabilities in the socio-technical system are rarely embodied simply in the technology or society alone; there are both structural and cultural vulnerabilities that need to be understood and "patched," so to speak. The work that we do in this initiative focuses primarily on addressing these vulnerabilities.

**Examples of current work include:**
*Data Voids* - Search engines are especially vulnerable to manipulation when there is limited data available for a particular search. Our work here seeks to better understand these data voids, how they are exploited, and how they can be patched.

*History of Security Research* - Examining technical systems to identify vulnerabilities was once the act of "hackers" who were often seen as adversarial even when they were probing systems to help strengthen them. Today, security research, penetration testing, and white hat hacking are seen as legitimate and

desired activities--economically incentivized in bug bounty programs and lucrative jobs. This project explores what technical and social changes made this possible.

*Bug Bounty Labor* - This project seeks to understand who participates in bug bounty programs and why. The goal is to understand bug bounty work and how these programs could provide models for efforts to produce more secure socio-technical systems.

*Socio-technical Threat Modeling* - In this work, we're looking to help stakeholders who are trying to secure socio-technical systems (i.e., communities) model the technical, communications, and data pollution threats in order to more effectively respond to emergent threats in real-time.

*Refractive Attacks* - In order to manipulate Google, it's often easier for an attacker to focus on Twitter, reddit, or Wikipedia. By understanding API and other information dependencies, we can see how vulnerabilities often occur in the interstices between technical systems.

*Dodging/Testing Guardrails* - Major technology companies have built numerous guardrails to identify when media manipulators are trying to exploit their systems, but some adversaries learn where these guardrails exist and exploit them. This is best seen through the lens of content moderation, where our team has examined different efforts to test and dodge restrictions.

**About the position**
We are looking for a researcher or postdoctoral scholar to join this team. This is a two-year open-level position, with pay commensurate with experience. At the junior end, we would be looking for a postdoctoral scholar or researcher with equivalent experience structuring a research project, conducting independent research, and producing scholarly outputs. At the more senior end, we would be looking for a seasoned scholar or researcher who also has experience mentoring junior scholars, an extensive publication track record, and a deep understanding of how to construct and support collaborative research teams.

Candidates are asked to propose a research project in the application, but should be open to co-constructing and iterating on their research agenda with other members of the team. Applicants will be assessed based on their track record as researchers, quality of writing samples, and proposal. Semi-finalists will be asked to interview via video. Finalists will be asked to give on-campus (or video) talks and engage in more extensive interviews.

The work we are seeking to support in this initiative should advance our collective understanding of the socio-technical vulnerabilities and the tools or processes that could help address them. We are primarily looking to understand structural vulnerabilities, where adversaries capitalize on weaknesses in how information, organizations, and institutions operate to pollute the information ecosystem and undermine trust in extant knowledge systems.

- This position is located at the Data & Society office in the Flatiron district of New York City.
- Remote candidates are also welcome to apply.

- You must be eligible to work in the United States. Data & Society is unable to sponsor visas at this time.
- You will be offered a generous benefits package including health insurance, paid time off (PTO), and paid holidays.

Salary: $72K - $100K (Commensurate to experience)

**To Apply, please submit the following materials by October 25th, 2019** (Applications will be reviewed on a rolling basis) by following the link here.

- Cover letter explaining why you are right for this role and your interest in working with Data & Society [Postdoctoral Scholar applicants, please describe your current research agenda, your dissertation topic, and your planned research and professional trajectory. Also, please indicate your desired start date and position length and when you received/will receive your PhD];
- CV;
- A one- to two- page proposal for a potential research project that you would like to pursue while at Data & Society (if you have multiple projects in mind, please feel free to send two distinct proposals). Your proposal should describe the research question, field site/data, methodology, and potential implications of doing this research project, as well as the connection to Data & Society's mission and research priorities;
- Writing sample (i.e. journal article, conference proceedings, book chapter, or equivalent;)
- The names, affiliations, and email addresses of three recommenders.

Applications will be reviewed on a rolling basis, and the position is considered open until filled. Please feel free to contact jobs@datasociety.net with any questions about the position. Questions about the opportunity or process will not reflect negatively on your application.

**About Data & Society**
The issues that Data & Society seeks to address are complex. The same innovative technologies and socio-technical practices that are reconfiguring society – enabling novel modes of interaction, new opportunities for knowledge, and disruptive business paradigms – can be abused to invade people's privacy, provide new tools of discrimination, and harm individuals and communities.

To provide frameworks that can help society address emergent tensions, Data & Society is committed to identifying thorny issues at the intersection of technology and society, providing and encouraging research that can ground informed, evidence-based public debates, and building a network of researchers and practitioners who can anticipate issues and offer insight and direction.

Data & Society's programming brings together different perspectives, research methods, and practices. We weave together researchers, entrepreneurs, activists, policy creators, journalists, geeks, and public intellectuals. We see tremendous reciprocal benefits for network building and research when they are combined.

The work and well-being of Data & Society are strengthened by the diversity of our network and our differences in background, culture, experience, national origin, religion, sexual orientation, and much more. We are committed to making certain that a wide array of perspectives are heard and that our research is

publicly available. We welcome applications from people of color, women, the LGBTQIA community, and persons with disabilities.