Carnegie Fellow Proposal of Peter Swire
November 17, 2017

"Protecting Human Rights and National Security in the New Era of Data Nationalism"

In this research program, I seek to study the new era of "data nationalism," the increasingly common actions by nations to control the flow of data, especially personal data, from one country to another. Data nationalism threatens fundamental human rights, when national control of the Internet reinforces surveillance and suppresses free speech. Data nationalism also threatens legitimate law enforcement and national security activities, where lawful cooperation among allies is undermined by protectionist limits on information sharing. The research would create research to reduce the risk of one-sided approaches to data nationalism, which threaten to lead to large ruptures of global data flows.

I. Problem Statement

In my research and government service, I have long sought to protect fundamental rights including privacy. In doing so, I have also sought to craft solutions that foster public safety and national security. These multiple goals were central to our work in drafting "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technology."

My ongoing research on global flows of personal information indicates that we are entering a new era of **"data nationalism,"** with sharply increasing actions by nations to control the flow of data, especially personal data, from one country to another. Prominent current examples include:

1. New laws in China (2017), Russia (2015), and potentially other major countries require **data localization**, to give governments ready surveillance access to communications. I have been studying the negative impact of data localization on human rights and free speech.
2. This fall, the Irish High Court certified the *Schrems v. Facebook* case to the European Court of Justice. The Irish Court held that there is a well-founded basis for believing that National Security Agency (NSA) surveillance is so pervasive in the U.S. that there is "inadequate" protection of the privacy rights of Europeans when their data is sent to the U.S. In the name of privacy protection, the decision may cause **large disruptions in international data flows**, but my research to date suggests that the decision may actually undermine privacy protection, while also creating risks to desirable information sharing among NATO allies.
3. This fall, the U.S. Supreme Court agreed to hear an appeal in a case where the U.S. Department of Justice is seeking evidence stored by Microsoft in Ireland. The case is an example of the increasingly acute battles between nations about how to get evidence stored overseas, such as emails stored in the cloud. In effect, the Department of Justice is seeking **sweeping new powers to acquire access to communications.** That outcome would be a variation of data nationalism, creating a precedent for nations to insist that data stored anywhere in the world be available to each nation's surveillance authorities.

The conflicts arising from data nationalism pose large risks to privacy and human rights. Under the globalized Internet that has existed to date, individuals and civil society organizations have adopted technical measures to protect their privacy and human rights activities, notably by encrypting their communications. Individuals and civil society have also adopted other measures that limited surveillance, such as choosing online service providers that store communications

outside of the reach of local authorities. Data nationalism measures are threatening this freedom from surveillance: nations including the United Kingdom have passed legislation to limit the effectiveness of encryption, and the new data localization measures are designed to help local governments implement surveillance more effectively.

The conflicts arising from data nationalism also pose large risks to the effectiveness of legitimate law enforcement and national security activities. Just as data nationalist rules can provide over-reaching powers for government surveillance, they can also they create rigid outcomes that limit legitimate government access to data under the rule of law. The E.U. is on the brink of cutting off many data flows to the U.S. based on its concerns about NSA activities, even though detailed scholarship shows that existing E.U. safeguards are in fact systematically less protective than U.S. practices. Protectionist pressures within nations can thus lead to economic disruptions, as well as unprecedented interruptions of information sharing among the intelligence and other activities of NATO allies.

Research and stakeholder engagement is urgently needed about how best to achieve the goals of (a) human rights protection and (b) national/international security in this new era of data nationalism. This project seeks to address these pressing problems.

II. The Research Project

The project would address the human rights and national security implications of data nationalism. **The research plan would apply to data nationalism an approach similar to the research program developed for the Georgia Tech Project on Cross-Border Government Access to Data.**[1] Since early 2015, I have led this project on Mutual Legal Assistance (MLA), with lead

[1] http://www.iisp.gatech.edu/cross-border-data-project.

funding from the Hewlett Foundation, which was successfully renewed for 2017-18. The MLA project has produced multiple articles and shorter papers. As with the proposed new inquiry into data nationalism, that project has addressed a rapidly emerging international set of issues that had not previously received systematic and effective academic and policy attention.

The data nationalism project would initially focus on insightful **description** of the multiple aspects of data nationalism. As with the MLA project, it is important to provide an accurate description of the key stakeholders, the incentives they face, and a neutral and accurate account of their views. Due to the complexity of the issues, the new descriptive material must be presented clearly and with academic credibility, in ways that can reach the multiplicity of relevant audiences. The research project would draw on the requisite, complex set of disciplines, including privacy, human rights, law enforcement, foreign intelligence, international law, and cybersecurity. This description will draw attention to emerging problems, notably the negative effects of new forms of data nationalism.

The new project would next **develop normative arguments** about how to proceed. For example, consider an article I am currently completing on "Understanding Why Citizenship Matters for Surveillance Rules," which I will present at two leading European conferences in January. This research illustrates the normative goal of finding nuanced approaches that uphold human rights, including privacy and the protection of democracy, as well as other pressing goals such as national security. To do so requires iterative vetting with policymakers, academics, and civil society as a form of validation.

The proposed research project would be for two years. In the second year, I would plan to host one or more conferences. I have a proven track record of running such conferences, such

as the 2017 conference at Georgia Tech for the MLA project.[2] That conference's proceedings were published in the widely read Lawfare blog, to reach a broad audience, including policymakers. To support the proposed research project, Georgia Tech has offered a greatly reduced cost for buying out of one course each year. The grant would pay a half-month of summer support to the PI and would substantially support a full-time researcher with a law degree and knowledge of diverse technical, policy, and legal topics.

III. Research Proposal and the Criteria for the Carnegie Fellows

The proposed research directly supports the objectives of the Carnegie call for proposals, by specifically focusing on the priority area: "global connections and global ruptures". Information sharing and continuing to foster the open Internet are central features to promoting "global connections." By contrast, data nationalism is a prominent new threat that may lead to substantial "global ruptures." In addition, the research project would assist in "strengthening US democracy and explore new narratives."

The project also meets the criteria for evaluation: (1) originality and promise of the idea; (2) quality of the proposal; (3) potential impact on the field; (4) record of the nominee; and (5) plans to communicate findings to a broad audience. My prior work shows a demonstrated record of national and global impact, with dissemination of findings to broad audiences. As with the prior work, the proposed research topic addresses original, pressing, and international issues. In short, the project would support research and workable proposals to reduce the risk of one-sided approaches to data nationalism, which threaten to lead to large ruptures of global data flows.

[2] http://cets.gatech.edu/news-2/surveillance-privacy-and-data-across-borders-transatlantic-perspectives.