Workshop program

MARIO EINAUDI
Center *for*
International Studies

Surveillance, Privacy, and Civil Society

February 12-13, 2018

ILR Conference Center

Cornell University

Organized by the Cybersecurity Working Group and cosponsored by Cornell Computing and Information Science, Cornell Law School, and the Judith Reppy Institute for Peace and Conflict Studies

WELCOME!

Ubiquitous computing and networking have provided many societal benefits, but they have also proliferated means of invading individual privacy, conducting mass surveillance, and otherwise influencing civil societies around the world. This workshop brings together legal, political, and technical experts from around the world to discuss these problems. We plan to publish an electronic book by Cornell University Press on the topic.

This conference is organized by the Cybersecurity Working Group and cosponsored by Cornell Computing and Information Science and Cornell Law School. The Cybersecurity Working Group is a collaborative project of the Einaudi Center, the faculty of Computing and Information Science, and the Judith Reppy Institute for Peace and Conflict Studies. Its overarching goal is to build a robust network and community around Cornell on international dimensions of cybersecurity.

We look forward to your participation!

Fred Schneider
Samuel B. Eckert Professor of Computer Science, Cornell University

Rebecca Slayton
Associate professor of science and technology studies, Cornell University

AGENDA

MONDAY, FEBRUARY 12

8:00 a.m. **Breakfast**

8:45 a.m. **Welcome and opening remarks**

Fred Schneider, Samuel B. Eckert Professor of Computer Science, Cornell University
Rebecca Slayton, associate professor of science and technology studies, Cornell University

LAW

9:00 a.m. **Government Access to Private Sector Data**

Fred Cate, Vice President for Research, Distinguished Professor, C. Ben Dutton Professor of Law, and adjunct professor of informatics and computing, Indiana University

9:45 a.m. **Governing Digital Life: The Challenge of Overlapping Regulatory Regimes**

Annelise Riles, Jack G. Clarke Professor of Law in Far East Legal Studies and professor of anthropology, Cornell University

10:30 a.m. **Coffee break**

11:00 a.m. **Understanding Why Citizenship Matters for Surveillance Rules**

Peter Swire, Nancy J. and Lawrence P. Huang Professor, Law and Ethics Program, Georgia Tech

11:45 a.m. **Data Portability and Information Fiduciaries**

Kunifumi Saito, assistant professor, faculty of policy management, Keio University

12:30 p.m. **Lunch**

CULTURE

1:30 p.m. **Myths and Fallacies of Personally Identifiable Information**

Vitaly Shmatikov, professor of computer science, Cornell Tech

MONDAY, FEBRUARY 12 (CONTINUED)

2:15 p.m. **Human-IT Ecosystem: A Nonhuman-Centric Approach to Managing Artificial Intelligence**

Jiro Kokuryo, vice-president of international collaboration, Keio University

3:00 p.m. **Against Privacy: The Dao of Surveillance – China's Regulatory Regimes on Cybersecurity**

Xingzhong Yu, Anthony W. and Lulu C. Wang Professor in Chinese Law, Cornell University

3:45 p.m. **Coffee break**

4:00 p.m. **Dashcams, Surveillance, and Privacy**

Takehiro Ohya, professor of jurisprudence, Keio University

4:45 p.m. **A Transnational Movement for Privacy? Securitization and the Protection of the Internet**

Sidney Tarrow, Maxwell M. Upson Professor Emeritus, Department of Government, Cornell University

5:30 p.m. **Break**

6:00 p.m. **Dinner**

Taylor Room, Statler Hotel

TUESDAY, FEBRUARY 13

8:00 a.m. **Breakfast**

CONCEPTS

8:30 a.m. **Privacy as Trust**

Keigo Komamura, Vice-President and professor of law, Keio University

9:15 a.m. **Privacy in a Networked Society**

Tatsuhiko Yamamoto, professor of constitutional law, Keio University Law School

10:00 a.m. **Coffee break**

TECHNOLOGY

10:15 a.m. **Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications**

Steve Bellovin, Percy K. and Vidal L. W. Hudson Professor of Computer Science, Columbia University

11:00 a.m. **The Ethics of Zero Day Exploits: The Trolley Car Meets Godzilla**

Steve Wicker, professor of electrical and computer engineering, Cornell University

11:45 a.m. **Network Traffic Obfuscation and Automated Internet Censorship**

Tom Ristenpart, associate professor, Cornell Tech

12:30 p.m. **Lunch**

1:30 p.m. **Closing remarks**

Fred Schneider, Samuel B. Eckert Professor of Computer Science, Cornell University
Rebecca Slayton, associate professor of science and technology studies, Cornell University

WORKSHOP THEMES AND ABSTRACTS

LAW

Government Access to Private Sector Data
Fred Cate

Governments increasingly turn to the private sector for data they previously would have sought through their own means. Why assign three teams of FBI agents in three cars to follow a suspect when you can just go to the phone company and track the suspect's location via cell towers? The effect is to make government surveillance cheaper, easier, and even possible after the fact – like going back in time. Edward Snowden first demonstrated the extent to which the U.S. government relies on the private sector for wholesale, systematic surveillance of large swaths of the population, but recent revelations have shown how much other countries engage in similar activities. Interestingly, government use of private sector data is often unregulated by privacy laws targeting government surveillance and by laws targeting the private sector. How should we be dealing with the issue of systematic government access to personal data held by the private sector?

Governing Digital Life: The Challenge of Overlapping Regulatory Regimes
Annelise Riles

Digital life crosses borders, and often even takes place without parties' awareness of the transnational nature of their interaction. In contrast, privacy and national security regimes are still largely territorially oriented. The result is that more than one jurisdiction can often legitimately claim authority over specific conduct. Debates about what to do about this condition have resulted in two standard positions. The first is that cyberspace is "nowhere," or at least not like any other territorial jurisdiction, and hence should not be thought of as subject to standard regulation. The second is that cyberspace can be territorialized and hence subject to regulation without considerable challenges. Neither of these positions gives us a compelling vision of how to address the specific qualities and challenges of digital life.

This presentation will focus on the example of differing resolutions of the tension between privacy and national security in the U.S. and Europe in the aftermath of the PRISM program in the U.S. and the ECJ decisions in Europe. To make this more concrete and give us something to discuss, I will unpack a hypothetical case of a French law student who joins a hypothetical California-based social media platform ("Handbook") in France. The user agreement specifies that Handbook will comply with all relevant national laws. He then moves to the U.S. to pursue a one-year degree and discovers that his Handbook account is now subject to U.S. government surveillance under the PRISM program. He sues Handbook in California, arguing that Handbook cannot share his data with the U.S. government under the PRISM program, even though he is voluntarily in the U.S., because it violates his fundamental rights as a European citizen. Cases like this raise larger theoretical questions about the nature of citizenship, the meaning of dignity and personhood, and the relationship of persons to states in a transnational world that is shaped (only in some respects) by digital technologies.

Understanding Why Citizenship Matters for Surveillance Rules

Peter Swire

This talk examines whether the nationality of an individual under surveillance (the "target") should be relevant to the legal standards for surveillance. The issue of target nationality arises as part of an increasingly important topic of international debate – the rules that apply to Mutual Legal Assistance (MLA), the ways that nations cooperate for accessing information held in other countries. In other writings, as part of the Georgia Tech Cross-Border Requests for Data Project, we have explained why the importance of MLA issues will continue to grow, notably due to what we call the "globalization of criminal evidence." The prevalence of online services, including webmail and social networks, means that evidence relevant to ordinary domestic crimes is increasingly stored by a service provider in another country. Most of the current reform proposals treat surveillance rules differently depending on the nationality of the target.

Data Portability and Information Fiduciaries

Kunifumi Saito

In the United States, some scholars recently developed the concept of "information fiduciaries" to protect individual privacy rights from huge online businesses. On the other hand, the European Union included an article on the "right to data portability" in the General Data Protection Regulation. The speaker will try to introduce some issues under Japanese law into the global context of consumer privacy.

CULTURE

Myths and Fallacies of Personally Identifiable Information

Vitaly Shmatikov

This talk addresses what "identity" and "anonymity" mean in different contexts, and why there is no universal notion of anonymity that can apply across the board, regardless of the person and scenario, and be technologically enforceable. It will also discuss what privacy might mean in an era of ubiquitous surveillance, and especially what it means to have privacy for personal communications given all we know about modern data collection and tracking technologies.

Human-IT Ecosystem: Nonhuman-Centric Approach to Managing AI

Jiro Kokuryo

Asia has a tradition of considering humans as part of, rather than at the top (or center) of an ecosystem. We must be mindful of such cultural diversity in designing governance mechanisms.

Against Privacy: the Dao of Surveillance – Comments on China's Regulatory Regimes on Cybersecurity

Xingzhong Yu

With the promulgation of a national law on cybersecurity and accompanying policies, strategies, administrative rules, and regulations, China is said to have entered an era of "Big Security," in which all Chinese citizens are expected to cooperate with the government in constructing a defensive network for cybersecurity. At the same time, the government has made good efforts to ensure the internet service providers, such as Wechat, Weibo by, Taobao, and JD.COM, comply with the privacy requirements provided by Chinese law. However, in a culture of pervasive surveillance inherited from traditional political consciousness and enhanced by posthuman technology, there still exist huge challenges to the adequate protection of the privacy of individual citizens by any means. China has yet to make a national law to protect personal information, and nongovernmental organizations need to find their role in cyberspace governance informed by multilateralism. This paper examines China's cybersecurity regulatory regime and related practice within the last decade, focusing on the dilemma between surveillance and protection of individual rights, especially the right to privacy. It questions the feasibility of a dialectical view of a proper balance between government surveillance and individual privacy in the context which lacks a third-party buffer zone of civil society and argues for more flexible collaboration of multiplayers in cyber governance.

Dashcams, Surveillance, and Privacy

Takehiro Ohya

While the "Dashcams," video recording devices stored on cars' dashboards to survey events happening in front of the vehicle, are very widely used in Japan, they are facing much resistance and privacy concern in European countries. The speaker will try to investigate this difference from various viewpoints, including cultural evaluation of privacy, trust of police, and other legal systems.

A Transnational Movement for Privacy? Securitization and the Protection of the Internet

Sidney Tarrow

Scholars and legal practitioners have long observed profound differences between the privacy practices of Europe and the United States. This has produced incompatible regimes of regulation, causing serious normative and political issues, culminating in the passage of the "Safe Harbor" agreement in 2000, which was meant to govern the exchange of commercial information across the Atlantic. But after 9/11, the gaps between Europe and America shrank as both Europe and the United States adopted increasingly intrusive security measures. This convergence was revealed by the Snowden affair in 2013. One effect of the Snowden revelations was the liquidation of "Safe Harbor" by the European Court of Justice; a second was the passage of a more robust EU General Data Protection Regulation; and a third was greater interaction and increased collective action on the part of European and American privacy advocates. This paper shows that this growing convergence may be producing incentives for the formation of a transnational movement to protect privacy on the Internet. The paper employs a "political opportunity structure" framework to understand how international events between 9/11 and the Snowden revelations securitized the monitoring of commercial and personal electronic communications and increased the density of the privacy advocacy network across the Atlantic.

CONCEPTS

Privacy as Trust

Keigo Komamura

Various concepts of privacy, such as the "right to be left alone," "autonomy or independence of personal space," or "the right to control personal information," have been developing in our modern society. Currently technology is pushing us to reconsider the concept again. In my talk, I will focus on a new view which understands privacy as "trust" and explore its theoretical and humanistic background, referring to its practical implications in Japan as well.

Privacy in Networked Society

Tatsuhiko Yamamoto

We have been embedded in a network system. We have no choice but to enter the system. Living within the system might be considered to be "the state of nature" or the baseline of our lives. I will try to think about whether and how we should change the concept of "privacy" in this new environment.

TECHNOLOGY

Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications

Steve Bellovin

Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels "going dark," these attempts to regulate security technologies on the emerging internet were abandoned. In the intervening years, innovation on the internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today, there are again calls for regulation to mandate the provision of exceptional access mechanisms. In this article, a group of computer scientists and security experts, many of whom participated in a 1997 study of these same topics, has convened to explore the likely effects of imposing extraordinary access mandates. We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force internet system developers to reverse "forward secrecy" design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.

The Ethics of Zero Day Exploits: The Trolley Car Meets Godzilla

Steve Wicker

The May 2017 WannaCry ransomware attack caused a great deal of damage across Europe and Asia, wreaking particular havoc with Britain's National Health Service. Cybersecurity analysts quickly found that the attack exploited a Microsoft Windows vulnerability that had been discovered, developed, and misplaced by the U.S. National Security Agency. The NSA informed Microsoft of the problem, but only after the NSA had lost control of the assets it had developed to exploit the vulnerability. In this talk, I consider whether U.S. government employees are behaving ethically when stockpiling software vulnerabilities. I briefly review the nature of these bugs and the resulting "zero-day" vulnerabilities and exploits, then proceed to a consideration of whether stockpiling is acceptable from an ethical standpoint. This is a difficult problem, as the standard consequentialist arguments on which current policy is based are crippled from the outset by security considerations. Such issues can be avoided by using a non-consequentialist approach. I conclude by showing that there are strong non-consequentialist arguments for the view that the stockpiling of vulnerabilities has no ethical support.

Network Traffic Obfuscation and Automated Internet Censorship

Tom Ristenpart

Internet censors such as China, Iran, and other nation-states seek ways to identify and block internet access to information they deem objectionable. Increasingly, censors deploy advanced networking tools such as deep-packet inspection (DPI) to identify such connections. In response, activists and academic researchers have developed and deployed network traffic obfuscation mechanisms. These apply specialized cryptographic tools to attempt to hide from DPI the true nature and content of connections. In this talk, I will give an overview of network traffic obfuscation and its role in circumventing internet censorship. I will discuss the historical and technical background that motivates the need for obfuscation tools, and give an overview of approaches to obfuscation used by state-of-the-art tools. Finally, I'll mention the latest research on how censors might detect these efforts.

ABOUT

Mario Einaudi Center for International Studies

The Einaudi Center was established in 1961 to enhance Cornell's research and teaching about the world's regions, countries, cultures, and languages. In 1990, it was named for its founding director, the political theorist Mario Einaudi. Today, the center houses area studies and thematic programs; organizes speaker series, conferences, and events; provides grants and other support to faculty and students; and brings together scholars from many disciplines to address complex international issues.

MARIO EINAUDI
Center *for*
International Studies

170 Uris Hall
Cornell University
Ithaca, NY 14853-7601 USA
t. 1 607 255 6370
f. 1 607 254 5000
einaudi_center@cornell.edu
www.einaudi.cornell.edu
twitter.com/einaudicenter
facebook.com/einaudicenter

Cornell University