Notes on Aaron Burstein,

“Conducting Cybersecurity Research Legally and Ethically”

Elliot Block

Prologue: legal versus ethical obligations
This lecture introduced the legal and ethical obligations involved in cybersecurity research. An important first step is to understand the difference between laws and ethics. According to Burstein, understanding one’s legal obligations is “a question with an answer, if you know the facts.” That is, legal obligations are knowable by examining the relevant codified standards, e.g. statutes, regulations and court decisions. Ethical obligations, however, are subject to a more “free-ranging inquiry.” Performing such an inquiry involves considering the interests of the researchers, subjects and institutions involved; ethics more generally comes down to thinking more about how your work affects other people. Focusing on the more tractable questions of law, the lecture mainly concerned itself imparting facts relevant to legal security research.

Introduction: historical context of research law
How does legal context affect research? The prime historical example is medical law. For hundreds of years, medical science has co-evolved with the law; laws arose to guard against abuse and irresponsibility, but researchers won exceptions in those laws to allow for the risk inherent in experimentation. Thus political competition resulted in a compromise that now allows for controlled scientific experimentation. In contrast to the long evolutionary history of medical law, cybersecurity law is young and unrefined: it arose in the 1960s to 1980s without the participation of a (then non-existent) network-security community, and consequently without many of the research provisions health researchers take for granted. Today cybersecurity researchers receive funding and attention from agencies such as congress, the National Science Foundation, and the Department of Homeland Security—but with the exception of emergencies and matters of national security, cybersecurity researchers have yet to receive allowances permitting the legal collection and publication of experimental data.
**Electronic Communications Privacy Act**
The Electronic Communications Privacy Act (ECPA) is the primary example of cybersecurity law. ECPA concerns the privacy standards for what and how one can monitor data legally—with the notable property that there are no research exceptions in ECPA. ECPA categorizes data along two dimensions: 1) content vs. non-content, and 2) real-time vs. stored.

The first distinction is between “content” and “non-content.” Content is considered the substance, purport, or meaning of a communication. This could be an IP packet’s payload, an e-mail subject line or a message body. Non-content is addressing information, such as to/from fields of a message, or an IP address. Together the content and non-content constitute the communication.

The second axis is real-time versus stored. As one might expect, this is the difference between watching a transmission while it is happening, as opposed to after it has reached an endpoint is waiting in storage. There are some tricky cases, however, such as e-mail. (See Real-time interception in the sidebar to the right.) ECPA’s two dimensions thus define four types of communication, each handled by a particular law.

The Wiretap Act and Pen/Trap Statute prohibit the monitoring of real-time content and real-time non-content information respectively. Two exceptions are court-ordered warrants and suspicion of foul play by a network operator. Even after the legal collection of data, however, the laws are restrictive about the legal disclosure of data. (See sidebar.)

The Stored Communications Act (SCA) addresses both stored content and stored non-content. Unlike Wiretap and Pen/Trap, SCA only applies to public ISPs; private companies like Google are not prohibited from reading the content you store with them, though they are prohibited from certain disclosures of content or non-content. These prohibitions, including those prohibiting giving data to the government, are looser and weaker than Wiretap and Pen/Trap—they evolved when catching abusers had to be done in real-time because data storage capacity was relatively insignificant.

**International privacy ideas**
The notion of privacy differs between the United States and Europe. The American conception of privacy originated from the desire to protect individuals from government intrusion. This resulted in tight restrictions on data disclosure to the government, but loose restrictions on private use. The European conception has more to do with a private life and free speech than governmental intrusion.

One illustrative example is data retention laws. European Internet Service Providers (ISPs) are required to retain data for law enforcement, while US ISPs are not.

In international incidents, legal obligations are primarily about the service’s location, rather than the user’s location. For example, an issue involving a French user an American service will be more about American law. Criminal law enforcement has the ability to coordinate internationally, but it is still at too small a scale to be an effective deterrent.

**Four types of information**
ECPA’s two dimensions define four types of communication, each of which is handled by a particular law.

1. Real-time content: Wiretap Act
2. Real-time non-content: Pen/Trap
3. Stored content: SCA
4. Stored non-content: SCA

**Real-time interception**
Matters of timing critically affect which laws an act falls under. *Interception* is the act of viewing a communication before its intended recipient views it.

The legality of monitoring is not only affected by who is monitoring, why they are monitoring, but also what they are monitoring. For example, monitoring telephone conversations is restricted to situations of suspected fraud or abuse, while computer networks are subject to looser controls.
Examples
Examples illustrated some of the legal and ethics considerations involved in security research.

Trace collection
A simple example considers the act of collecting of network activity data and potentially sharing it. The central issue is communications privacy. Legally there are restrictions on who, what and why one could collect this data, as defined in ECPA. Ethically, Burstein cited the factor of embarrassment and “respectful uses of published data.” In particular, if trace data reveals activity of users it is liable to embarrass one’s own organization, a remote institution, or individuals.

What are some ways to get trace data as a researcher? The first way is to attempt to get the consent of users. This tends to pose problems because individual consent is difficult to get and group consent often reveals little detail. An alternate possibility is to try to leverage the service provider exception, which allows network operators to monitor their own networks for defense purposes, but this requires collaborating with a service provider’s operational staff.

Trace disclosure
In general, the SCA is the law relevant to sharing or publishing packet traces. Disclosing full packet traces is prohibited without consent or a subpoena, but sharing packet header traces is allowed—unless they’re given to a “government entity.” Government entities are broader than law enforcement, including other public organizations such as public universities. Note that this disallows general public release, since a government entity could obtain the data. Other loopholes and considerations include:

- SCA applies only to “public” service providers, such as commercial ISPs, but not businesses, who have a freer legal license to monitor their employees, though ethical questions remain.
- The legal status of disclosing network activity data is different depending upon whether the activity occurs over one’s own network, versus someone else’s network. However, defining whose network the attack occurs on is difficult, especially if one finds oneself in the middle of a traffic or attack path, rather than at the endpoints.

Honeypots
Honeypots are computers that allow intentionally allow themselves to be infected, in order to study the activities of malicious software. The relevant law is the Computer Fraud and Abuse Act (CFAA). There are several stages of activity: collection/infection, communication and participation in attacks. That is, modern malicious software not only infects to destroy its target, but also infects in order to steal data or control the infected system for the attacker’s purposes. The passive stages of being infected are not forbidden, but the active stages of knowingly allowing one’s own computer to participate in malicious activities are legally problematic.

End