

DIGITAL SECURITY FOR ACTIVISTS



MARCH 2, 8PM EST.

A FREE TRAINING FROM JEWISH VOICE FOR
PEACE AND THE NATIONAL LAWYERS GUILD

Devin McDougall and Ken Montenegro

March 2, 2017

Talk Roadmap

- I. Key Digital Security Concepts
 - A. Assessing Risk
 - B. Constitutional Law Basics
- II. Case Study: Cell Phone Privacy
 - A. Legal Issues
 - B. Tech Issues
- III. Case Study: Borders and Airports
 - A. Legal Issues
 - B. Tech Issues
- IV. Questions and Answers

I. Key Digital Security Concepts

A. Assessing Risk

Why are we having this conversation?

- Fear
- Mis-information
- Safety



Assessing Risk

It's not rocket science; it's something traditionally targeted communities do on the daily.

- What's our context
- What do we want to protect
- Why do we want to protect it
- What happens if it gets out/disclosed/taken
- What are we willing to do to protect it
- Will we know if it's taken

Context Matters

- What are you working on?
- What is the political climate?
- Who are the political players (includes nonprofits)?
- What local knowledge do you have at your disposal/advantage?

B. Constitutional Law Basics

Constitutional Law Concepts

- Constitutional Law Basics
 - Bill of Rights created to limit the power of a strong federal government by protecting individual rights
 - Also applies to state and local governments
- Fourth Amendment
 - Affects whether the government can search your phone
- Fifth Amendment
 - Affects whether the government can compel you to provide a passcode or fingerprint

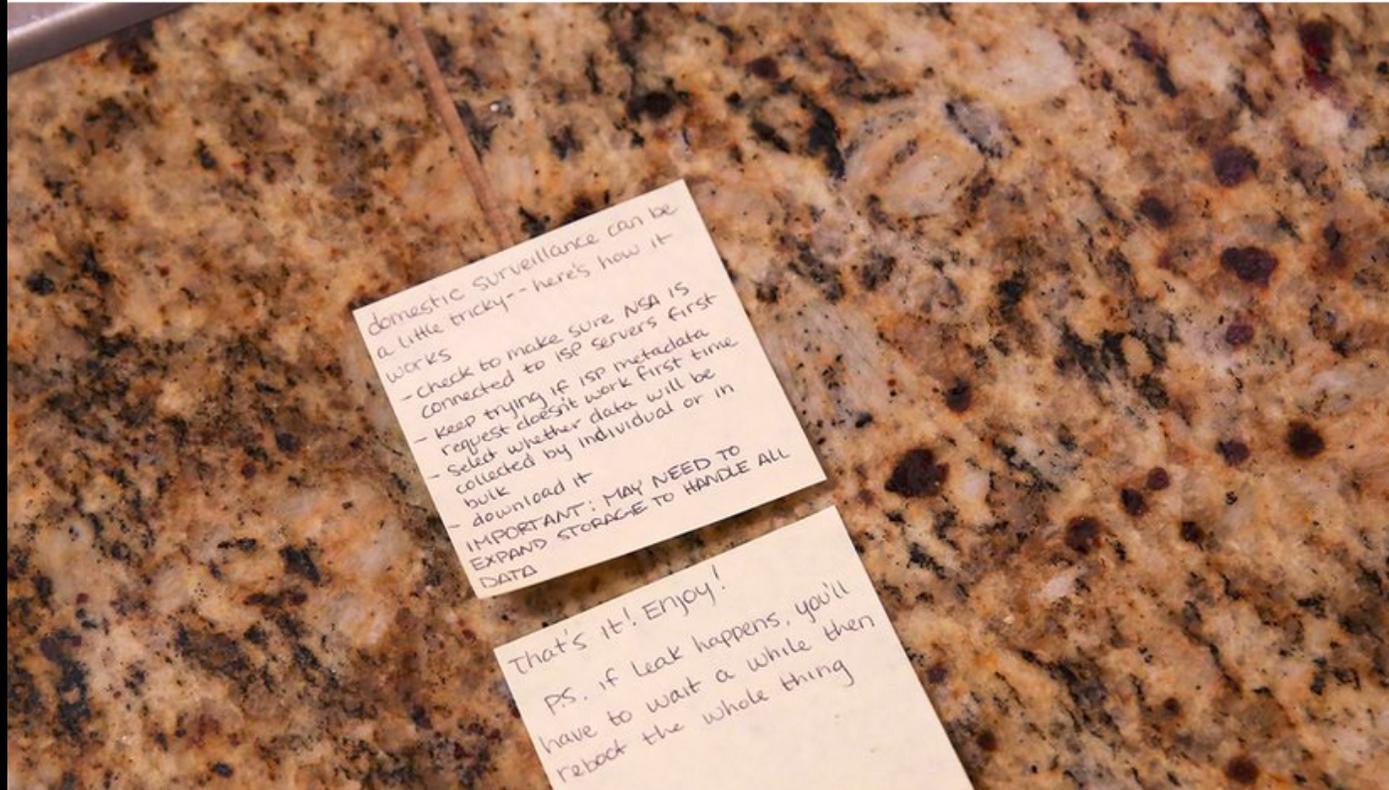
Important to remember: Constitutional law is made from the bottom up

- Law comes from the bottom up. Official law is influenced, often decisively, by what goes on in communities subject to their commands. What officials say is law neither exhausts the subject nor ends debate.
- Choice of law is not neutral. It is deeply ideological, generational, and subject to shift in response to changed circumstances.
- Our obligation to obey the law is based upon its normativity and not just its official pedigree. Every time the polity tries to suppress a vision of law, it risks its legitimacy, because it risks alienating groups whose vision has been suppressed.

William N. Eskridge, Jr. "Public Law From the Bottom Up,"
97 W. Va. L. Rev. 141 1994-1995

Elected officials don't necessarily have your back

Obama Leaves Post-It On Counter With Quick Note Explaining How To Use Extralegal Surveillance Apparatus



Courts don't necessarily have your back

 the ONION®

NEWS · 3.17.09 VOL 45 / ISSUE 12

Right To Privacy Not Guaranteed By Constitution, Says Supreme Court Justice Peeking In Bathroom Window

 WESTON, FL—In a public ruling made this week while peering into the home of 28-year-old resident Laura Daltry, Supreme Court Justice Samuel Alito stated that "in no way whatsoever" is the right to privacy explicitly upheld by the U.S. Constitution.



But “law is made from the bottom up”

- You (and your attorney) can make strong, principled rights-based arguments that are rooted in our Constitutional traditions
- This can, over time, help shift “the arc of justice” in a more progressive direction
- Constitutional law does change over time
 - *Brown v. Board of Education* (1954) overturned *Plessy v. Ferguson* (1896)
 - Fourth Amendment (ratified as part of Bill of Rights in 1791) not held to apply to state governments until 1961

Fourth Amendment

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

Fourth Amendment

- A “search” occurs for purposes of the Fourth Amendment when the government violates a person's “reasonable expectation of privacy”
- Searches must be “reasonable”
- Reasonable generally means:
 - Authorized by a warrant from a judge, which has been obtained by the government after a showing of “probable cause” that the search will reveal information relevant to a criminal investigation
- However, there are exceptions to the warrant/probable cause requirement:
 - Search incident to arrest
 - Plain view
 - Border searches – more on this later

Probable Cause

“Basic to search warrant protections is the requirement of probable cause. Its function is to guarantee a substantial probability that the invasions involved in the search will be justified by discovery of offending items.

Two conclusions necessary to the issuance of the warrant must be supported by substantial evidence: that the items sought are in fact seizable by virtue of being connected with criminal activity, and that the items will be found in the place to be searched.”

28 U.Chi.L.Rev. 664, 687 (1961)

Fifth Amendment

“No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”

Fifth Amendment

- Testimonial concept
- For passwords, showing your control over a device as distinct from the mere information required to access it
- Courts have analyzed the Fifth Amendment implications of being compelled to supply a passcode versus biometric information (such as fingerprints) differently

Model Rules of Professional Conduct

- “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”
Rule 1.6(c)
- “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”
Rule 1.1, Comment 8

Talk Roadmap

- I. Key Digital Security Concepts
 - A. Assessing Risk
 - B. Constitutional Law Basics
- II. Case Study: Cell Phone Privacy
 - A. Legal Issues
 - B. Tech Issues
- III. Case Study: Borders and Airports
 - A. Legal Issues
 - B. Tech Issues
- IV. Questions and Answers

II. Case Study: Cell Phone Privacy

A. Legal Issues

Legal Issues

- 1. Searching a phone
 - Fourth Amendment
- 2. Unlocking a phone
 - Fifth Amendment

In Re Application for a Search Warrant (2017)

- Case No. 17M081, U.S. District of N.D. Illinois, Magistrate Judge M. David Weisman
- Search warrant application seeks authority to search a premises and to seize any person present at a premises and compel them to provide their fingerprints for access to any Apple device found at the premises
- The basis for probable cause cited is evidence of child pornography downloads on the wifi network at the premises

In Re Application for a Search Warrant (2017)

- Court finds probable cause for a search of the premises and seizures of the devices
- Court denies order to compel fingerprinting
 - Court finds that under Fourth Amendment, seizing any person at the premises and compelling their fingerprinting is unreasonable without a showing of their connection to the crimes alleged
 - Court finds that Fifth Amendment right against self-incrimination protects individuals from being forced to show their ownership or control of any device found at the premises

Fifth Amendment, Fingerprints, and Passcodes

- If a device is known to be owned or controlled by a particular person, there is authority for a judge to issue an order compelling them to provide fingerprints to access it
- However, where the act of providing fingerprints will serve to establish a link between a person and a device, there is more Fifth Amendment protection against self-incrimination available
- Nevertheless, passcodes are a better choice for phone locking, because there is more authority for the view that being compelled to provide a passcode would be a forced testimonial act that the Fifth Amendment protects against
- Nonetheless, courts don't agree on whether passcodes can be compelled: VA (no) v. FL (yes)

Two recent back-to-back news stories...

Judge Rules Against Forced Fingerprinting (thestack.com)

Posted by BeauHD on Thursday February 23, 2017 @06:40PM from the you-always-have-a-choice dept.

An anonymous reader quotes a report from The Stack:

A federal judge in Chicago has ruled against a government request which would [require forced fingerprinting of private citizens](#) on their smartphones and tablets. [In the ruling](#), the judge stated that while fingerprints in and of themselves are not protected, the government's method of using them to search for evidence on these devices violates the Fourth and Fifth amendments. The government's request was given as part of a search warrant related to a child pornography case, but that it could not compel people physically present at the time of seizure to provide their fingerprints "on any other Apple brand device in order to gain access to the contents of any such device."

The report mentions that the ruling was based on three separate arguments. "The first was that the boilerplate language used to address vulnerabilities associated with wireless services. Second, the court said that the context in which the fingerprints were used violated the Amendment search and seizure rights of the building residents and their visitors, all of whom would have been compelled to provide fingerprints. Finally, the court noted that historically the Fifth Amendment, which protects against self-incrimination, does not allow a person to be compelled to provide fingerprints." [read more about the ruling via Ars Technica.](#)

[f](#) [t](#) [in](#) [g+](#) [AS](#)

Cellebrite Can Now Unlock Apple iPhone 6, 6 Plus (cyberscoop.com)

Posted by BeauHD on Thursday February 23, 2017 @06:00PM from the here-we-go-again dept.

[Patrick O'Neill](#) writes:

A year after the battle between the FBI and Apple over [unlocking an iPhone 5s](#) used by a shooter in the San Bernardino terrorist attack, Cellebrite [announced](#) it can [now unlock the iPhone 6 and 6 Plus](#) for customers at rates ranging from \$1,500 to \$250,000. The company also [announced](#) it can analyze data from a wide range of popular apps including all of the most popular secure messengers around.

From the Cyberscoop report: "Cellebrite's ability to break into the iPhone 6 and 6 Plus comes in their latest line of product releases. Cellebrite [boasts](#) dozens of new and improved features including the ability to extract data from 51 Samsung Android devices including the company's flagship models for Android's most popular brand, as well as the new high-end Google Pixel Android devices."

B. Tech Issues

Lock your devices!



Update your software (operating systems & applications)



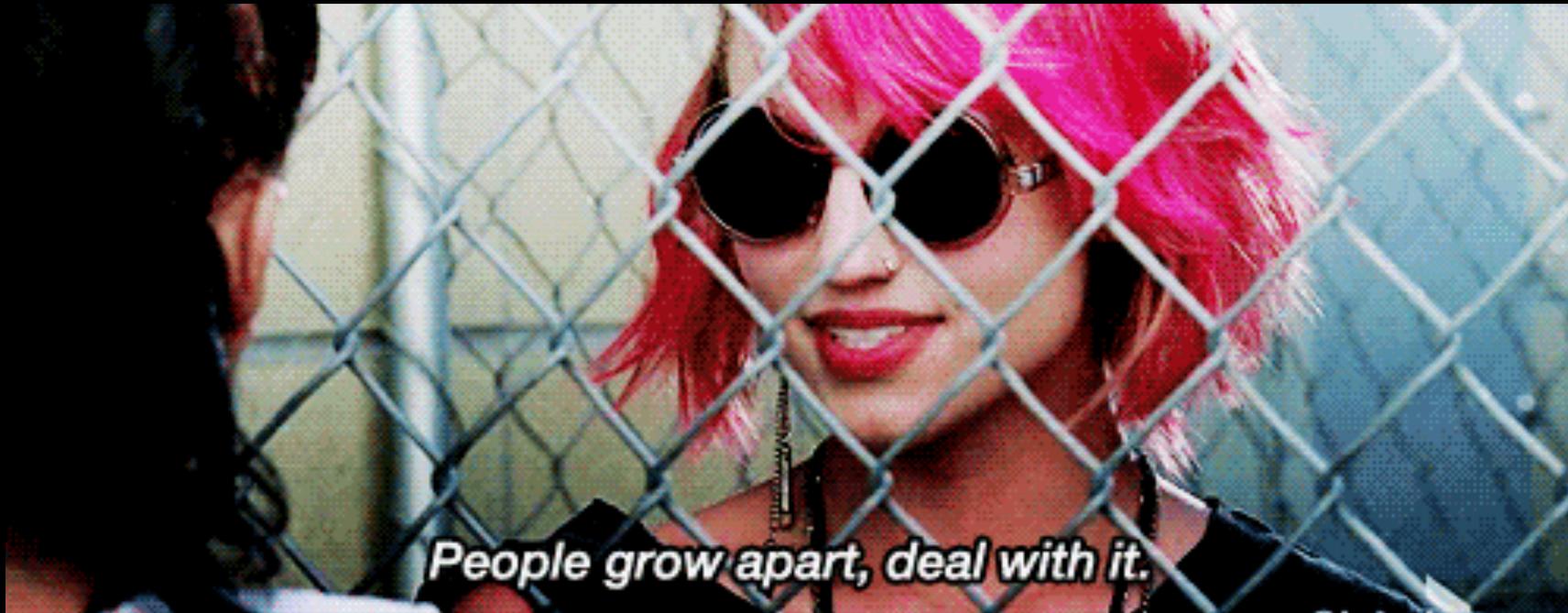
Use a password manager & don't recycle passwords



Practice secure text messaging & phone calls with Signal



Segregate work data from personal data



People grow apart, deal with it.

Talk Roadmap

- I. Key Digital Security Concepts
 - A. Assessing Risk
 - B. Constitutional Law Basics
- II. Case Study: Cell Phone Privacy
 - A. Legal Issues
 - B. Tech Issues
- III. Case Study: Borders and Airports
 - A. Legal Issues
 - B. Tech Issues
- IV. Questions and Answers

III. Case Study: Borders and Airports

A. Legal Issues

Fourth Amendment

- Border search exception: allows searches and seizures at international borders and their functional equivalent without a warrant or probable cause
- Varying positions of non-citizens, persons with provisional status, and citizens with respect to rights and practical capacity to push back
- Electronic devices and passwords
- Issue: identification checks on domestic flights

B. Tech Issues

Buenaventura Durruti said, “*I believe, as I always have, in freedom. The freedom which rests on the sense of responsibility.*” Security culture is an act of responsibility to clients, the broad NLG community, “the community”, partners, allies, & movements.



Talk Roadmap

- I. Key Digital Security Concepts
 - A. Assessing Risk
 - B. Constitutional Law Basics
- II. Case Study: Cell Phone Privacy
 - A. Legal Issues
 - B. Tech Issues
- III. Case Study: Borders and Airports
 - A. Legal Issues
 - B. Tech Issues
- IV. Questions and Answers

IV. Questions?

Questions?

Feel free to reach out if you have any further questions:

Devin McDougall – devin@devinmcdougall.org

Ken Montenegro – kmontenegro@advancingjustice-la.org