Week 2: CCTV and other surveillance tech in libraries

Real time lecture: June 13, 8:30 am Pacific/11:30 am Eastern

Overview

Surveillance technology like closed circuit television cameras (CCTV) are widely in use in libraries, yet their efficacy is debatable, and their procurement methods are often opaque. This week we'll talk about surveillance technology in libraries and our broader communities, discussing research about their efficacy as crime deterrents, as well as how their footage is used by law enforcement. We'll hear from Kade Crockford of the ACLU of Massachusetts on what librarians should know about CCTV, how we can build democratic processes around surveillance technology acquisition in our communities, and how to create policies around surveillance tech that can actually keep our communities safe.

Learning objectives

- Learn criticisms of CCTV use and efficacy
- Learn about surveillance technology acquisition methods
- Learn how to create policy around CCTV acquisition and use

Readings

- Video Surveillance in Public Libraries: a Case of Unintended Consequences?: http://www.academia.edu/2395122/Video_Surveillance_in_Public_Libraries_a_Case_of_Unintended_Consequences
- Silicon Valley startup that wants to put cameras in your neighborhood: https://www.mercurynews.com/2017/09/03/early-stage-this-surveillance-tartup-wants-put-cameras-your-neighborhood/
- School CCTV system broadcast publicly because they didn't change the default passwords: http://www.dailymail.co.uk/news/article-5432769/School-CCTV-systems-hacked-broadcast-online.html
- [optional] The Panoptic Librarian: The Role of Video Surveillance in the Modern Public Library https://www.ideals.illinois.edu/bitstream/handle/2142/47307/132_ready.pdf

Guest lecturer

Kade Crockford, Director of the Technology for Liberty program of the ACLU of Massachusetts
https://aclum.org/about/staff-advocates/kade-crockford/

Discussion

- Explore philosophically the concept of security -- who does surveillance tech make secure? Who does it make insecure?
- Is there a disconnect between CCTV efficacy and our policies? Between CCTV and library ethics?
- Is your library using CCTV? Where does the feed go? Who has access? How long is the data stored?

- How would you respond to arguments in favor of CCTV?
- What arguments can we make against CCTV? How can we redirect the conversation so it's still about safety?

Assignment

- Work with other LFI participants to begin drafting a CCTV policy. It doesn't need to be finished this week! But it could begin to explore the components that make a good one, eg who controls the information, who has access to the information, how it's stored, how it's acquired, when it's deleted, etc; or
- Write a one page plan on how you'd organize a democratic information session about surveillance tech in your community; or
- Write one page about how to find out if surveillance tech procurement is happening in your community and how to disseminate this info to patrons

Week 3: Tech tools basics // intro to teaching privacy

Real time lecture: June 20, 8:30 am Pacific/11:30 am Eastern

Overview

Better technology isn't the only step towards taking back privacy, but it's one of the most important and one of the few things we'll learn that can be implemented right away. This week we'll get a grounding in some important basic privacy tech tools and strategies with a guest lecture from a veteran privacy and security trainer, Rosalie Tolentino.

Some of what we'll cover this week includes:

- Software updates
- Passwords and password managers
- Full disk encryption
- HTTPS
- Malware and phishing prevention
- Introduction to privacy-protective tools

We'll also begin thinking about how to teach these strategies and tools to our communities.

Learning objectives

- Starting points for privacy tech instruction
- Strategies for incorporating tools into existing classes in inclusive ways

Readings

- Browse through EFF's Security Education Companion: sec.eff.org
- Learn about making secure passphrases with the Diceware method: https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/
- More on the Diceware method using EFF's wordlist: https://www.eff.org/dice
- Browse Tactical Technology Collective's Security-in-a-Box https://tacticaltech.org/projects/security-in-a-box-key-project/

Guest lecturer
Rosalie Tolentino of ThoughtWorks

Discussion

- How would you begin to bring these tools into the library?
- What about teaching to low literacy (digital or otherwise) patrons?
- What advice can you find in the Security Education Companion for teaching specific groups of patrons?

Assignment

- Make a diceware passphrase and write an instructional flyer (for library staff or patrons) about making stronger passwords and storing them; or
- Make an instructional flyer for the library about another one of these concepts; or
- Make three instructional slides on several of these concepts, focused on low digital literacy patrons; or
- Teach two people about some of what you learned (fellow library staff or patrons) and write one page about your experience -- what went well? How could you improve?

Week 4: You are the product: giant internet companies and how they threaten privacy

Real time lecture: June 27, 8:30 am Pacific/11:30 am Eastern

Overview

The internet is no doubt a democratizing force, amplifying the voices of individuals and communities that politically and economically disenfranchised and helping give rise to new media that propels new economic opportunities, creativity, and new social movements. It's how we communicate with loved ones, find jobs, and know what's happening around the world and in our communities. But for all its promise and all that we've come to depend on it for, the internet is under the control of a small handful of private companies, accountable to none but their shareholders. These few private companies, like Google and Facebook, shape the internet in ways that serve their bottom line—largely offering a "free" service in exchange for collecting vast amounts of data on their users. Business as usual relies that trove of user data, usually exploited

to send hyper-targeted and often manipulative advertisements to people based on their race, age, gender, religion, income level, and sexual orientation, and much of it is obtained without meaningful consent. The recent scandal with Facebook and Trump's voter targeting firm, Cambridge Analytica, is a prime example of how largely unregulated corporations online, can abuse private user data sway elections and reshape the world. This week's guest lecturer April Glaser, a journalist at Slate, will tell us more about how the economics of corporate data collection, what is and isn't happening politically to rein powerful internet giants in, and the myriad harms that data profiling has long had on vulnerable and marginalized communities online.

Learning objectives

- Understand ethical/privacy issues of major tech and internet companies
- Learn about the regulatory and political environment—and the lack thereof
- Discuss harm reduction strategies for using their platforms
- Craft strategies to incorporate this information into library instruction*

Readings

- The Cambridge Analytica Scandal Is What Facebook-Powered Election Cheating Looks Like: https://slate.com/technology/2018/03/the-cambridge-analytica-scandal-is-what-facebook-powered-election-cheating-looks-like.html
- Facebook (Still) Letting Housing Advertisers Exclude Users by Race: https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin
- Facebook Enabled Advertisers to Reach "Jew Haters": https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-hater
- 'Pro-Beyoncé' vs. 'Anti-Beyoncé': 3,500 Facebook ads show the scale of Russian manipulation: https://www.washingtonpost.com/news/the-switch/wp/2018/05/10/here-are-the-3400-facebook-ads-purchased-by-russias-online-trolls-during-the-2016-election/?utm_term=.abb96101981f
- Digital Inclusion and Data Profiling (highly recommended): http://firstmonday.org/article/view/3821/3199#11
- How Facebook Outs Sex Workers: https://gizmodo.com/how-facebook-outs-sex-workers-1818861596
- Facebook recommended that this psychiatrist's patients friend each other: https://splinternews.com/facebook-recommended-that-this-psychiatrists-patients-f-1793861472
- We read every one of the 3,517 Facebook ads bought by Russians. Here's what we found: https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/
- Google Was Right to Fire the Memo Writer: http://www.slate.com/articles/technology/technology/2017/08/why_did_a_google_engineer_feel_empowered_to_share_his_sexist_memo.html
- What will an Internet Without Net Neutrality Be Like?: http://www.slate.com/articles/technology/future_tense/2017/12/what_the_internet_is_like_in_countries_without_net_neutrality.html
- Facebook's Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children: https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms

- https://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout/

More Facebook/Cambridge Analytica pieces

- https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump
- https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-execs-boast-of-role-in-getting-trump-elected
- https://slate.com/technology/2018/04/why-arent-privacy-groups-fighting-to-regulate-facebook.html
- https://slate.com/technology/2018/04/facebook-collects-data-on-non-facebook-users-if-they-want-to-delete-it-they-have-to-sign-up.html
- https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie
- https://www.washingtonpost.com/business/economy/facebooks-rules-for-accessing-user-data-lured-more-than-just-cambridge-analytica/2018/03/19/31f6979c-658e-43d6-a71f-afdd8bf1308b_story.html

On the politics and culture of the world's most powerful internet
Companies:

- https://www.wired.com/story/how-trump-conquered-facebookwithout-russian-ads/
- http://www.slate.com/articles/technology/technology/2017/12/under_eric_schmidt_google_evolved_from_don_t_be_evil_to_be_kind_of_evil.html
- https://www.buzzfeed.com/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data?utm_term=.eoOLGv0vZ0#.jiLkMRJRnJ
- https://slate.com/technology/2018/03/the-exit-of-alex-stamos-reveals-a-troubling-debate-within-facebook.html
- https://www.buzzfeed.com/blakemontgomery/youtube-has-deleted-hundreds-of-thousands-of-disturbing?utm_term=.gnyqmxyxZy#.lhw2ZKoKno

Guest lecturer

April Glaser, tech journalist at Slate [https://twitter.com/aprilaser]

Discussion

- Discuss the business model of the internet and how corporations profile their the unfathomable amounts of user data they collect to serve manipulative and targeted ads
- Discuss the major issues -- data collection, insecure storage of corporate data (eg Equifax), sharing with law enforcement, the dangers of targeting ads based on stereotypes, voter manipulation
- How were these sites allowed to grow unchecked for so long? What kinds of policy interventions are possible?

- Discuss the assignment together (see below)

Assignment

- Write 3-5 talking points about what we discussed this week. Think of ways you could incorporate all or some of those points into instruction that would work at your library.
- Incorporate some of this information into instruction or outreach that works for your library. This could be anything from bringing it up at a staff meeting or talking to a patron directly. Write down what you did and how it went.

Week 5: “Threat modeling” and everyday privacy

Real time lecture: July 3, 8:30 am Pacific/11:30 am Eastern

Overview

A great deal of the conversation about privacy focuses on protecting people like journalists, whistleblowers, activists, and others whose adversaries might include powerful law enforcement or intelligence entities. But those are hardly the people at serious risk of having their privacy violated. This week, Eva Galperin of EFF will join us to talk about privacy threats that come from more personal relationships -- our classmates, family, bosses, and others who might be members of our communities. We’ll also introduce the concept of threat modeling -- a method of determining how a person should protect themselves based on who they are and who their adversaries might be.

Readings

- EFF’s guide to threat modeling: https://ssd.eff.org/en/module/assessing-your-risks
- Surveillance begins at home (domestic violence and privacy): https://www.forbes.com/sites/sarahjeong/2014/10/28/surveillance-begins-at-home/#1e809a2b7f41
- Browse through EPIC’s resources on domestic violence and privacy: https://www.epic.org/privacy/dv/
- That time the NSA used their surveillance tools to spy on their romantic partners: https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/
- Companies are using big data to predict worker illness, and other dystopian horrors: https://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940?mod=e2tw

Guest lecturer

Eva Galperin, Director of Cybersecurity at Electronic Frontier Foundation (https://en.wikipedia.org/wiki/Eva_Galperin)

Discussion

- Discuss threat modeling and its application in libraries

- Discuss the threat models we talked about this week. How do they apply to our communities?

Assignment

- Create an example threat model
- Write up a strategy for incorporating threat modeling in library instruction (either as a couple of slides or a plan to incorporate it into other instruction)