Bohyun Kim

Cybersecurity and digital surveillance versus usability and privacy[1]

Why libraries need to advocate for online privacy

Cybersecurity is an interesting and important topic, one closely connected to those of online privacy and digital surveillance. The Internet was invented to share things with others quickly, and it excels at that job. On the other hand, keeping private information safe and secure online is a challenging task. We have all heard of recent security breaches at J. P. Morgan, Target, Sony, Anthem Blue Cross and Blue Shield, the Office of Personnel Management of the U.S. federal government, University of Maryland-College Park, and Indiana University.

Sometimes a data breach takes place when an institution fails to patch a hole in its network systems. Sometimes, people fall for a phishing scam, or a virus in a user's computer infects the target system. Other times, online companies compile customer data into personal profiles. The profiles are then sold to data brokers, companies that collect personal information about consumers and then sell that data to other companies, and malicious hackers and criminals.

Cybersecurity versus usability

To prevent such a data breach, institutional IT staff are trained to protect their systems against vulnerabilities and intrusion attempts. Employees and end users are educated to be careful when dealing with institutional or customers' data. There are systematic measures that organizations can implement, such as two-factor authentication, stringent password requirements, and locking accounts after a certain number of failed login attempts.

These measures strengthen an institution's defense against cyberattacks, but they may also negatively affect the usability of the system, lowering users' productivity. For instance, security measures like a CAPTCHA can cause an accessibility issue for people with disabilities. Or imagine that a university IT office concerned about the data security of cloud services starts requiring all faculty, students, and staff to use only cloud services that are SOC 2 Type II certified. SOC stands for "Service Organization Controls," and it consists of a series of standards that measure how well a service organization keeps its information secure. For a business to be SOC 2 certified, it must demonstrate that it has sufficient policies and strategies that will satisfactorily protect its clients' data in five areas known as "Trust Services Principles," which include the security of the service provider's system; the processing integrity of this system; the availability of the system; the privacy of personal information that the service provider collects, retains, uses, discloses, and disposes of for its clients; and the confidentiality of the information that the service provider's system processes or maintains for the clients.[2] Dropbox for Business is SOC 2 certified,[3] but it costs money. The free version is not as secure, but many

Bohyun Kim is associate director of library applications and knowledge systems at the University of Maryland-Baltimore, Health Sciences and Human Services Library, email: bkim@hshsl.umaryland.edu

faculty, students, and staff in academia use it frequently for collaboration. If a university IT office bans people from using the free version of Dropbox without offering a compelling alternative, they could be affected negatively.

Another example of poor usability caused by security concerns is the website of the United States Postal Service. The USPS website does not provide a way to reset the password for users who have forgotten their usernames. They are instead asked to create a new account. Furthermore, if a user who remembers the account username enters wrong answers to the two security questions more than twice, the system automatically locks the account for a certain period of time. Again, a user is forced to create a new account. Clearly, a system that does not allow the password reset for those forgetful users is more secure than the one that does. However, in reality, this security measure creates a huge usability issue because average users do forget their passwords and the answers to the security questions that they set up themselves. It's not hard to guess how frustrated people will be when they realize that they entered a wrong mailing address for mail forwarding and find themselves unable to get back into the system to correct it because they cannot remember their passwords nor the answers to their security questions.

To give an example related to libraries, a library may decide to block all international traffic to their licensed e-resources to prevent foreign hackers who have gotten hold of a legitimate user's username and password from accessing those e-resources. This would certainly help libraries to avoid a potential breach of licensing terms in advance and spare them from having to shut down compromised user accounts one by one whenever they are discovered. However, this would make it impossible for legitimate users traveling outside of the country to access those e-resources, as well, which they would find unacceptable. Furthermore, malicious hackers would simply use a proxy to make their IP address appear to be located in the United States.

What would users do if their organization required them to reset passwords on a weekly basis for their work computers and several or more systems that they also use constantly for work? While this may strengthen the security of those systems, it's easy to see that it will be a nightmare having to reset all those passwords every week and keeping track of them. Most likely, they will start using less complicated passwords or even begin to adopt just one password for all different services. Some may even stick to the same password every time the system requires them to reset it unless the system forbids it. Ill-thought-out cybersecurity measures can easily backfire.

Security is important, but users also want to be able to do their job without being bogged down by unwieldy cybersecurity measures. The more user-friendly and the simpler the cybersecurity guidelines are to follow, the more users will observe them, thereby making networks and systems more secure. Users who face cumbersome and complicated security measures may ignore or try to bypass them, increasing security risks.

Cybersecurity versus privacy

Usability and productivity may be a small issue, however, compared to the risk of mass surveillance resulting from aggressive security measures. In 2013, *The Guardian* reported that the communication records of millions of people were being collected by the National Security Agency (NSA) in bulk, regardless of suspicion of wrongdoing and that a secret court order prohibited Verizon from disclosing the NSA's information request.[4] After a cyberattack against UCLA, the University of California system installed a device that is capable of capturing, analyzing, and storing all network traffic to and from the campus for more than 30 days. This security monitoring was implemented secretly without consulting or notifying the faculty and those who would be subject to the monitoring. The IT staff who installed

the system were given strict instructions not to reveal it was taking place,[5] and selected committee members on the campus were told to keep this information to themselves.[6]

The invasion of privacy and the lack of transparency in these network monitoring programs has caused great controversy. Such wide and indiscriminate monitoring programs must have a very good justification and offer clear answers to vital questions such as what exactly will be collected, who will have access to the collected information, when and how the information will be used, what controls will be put in place to prevent the information from being used for unrelated purposes, and when and how the information will be disposed of.

This year we saw another case in which security concerns conflicted with people's right to privacy. In February, the FBI requested Apple to create a backdoor application to bypass the current security measure in place in its iOS. This was because the FBI wanted to unlock an iPhone 5c recovered from one of the shooters in San Bernadino attack. Apple iOS secures users' devices by permanently erasing all data when a wrong password is entered more than ten times, if people choose to activate this option in the iOS setting. The FBI's request was met with strong opposition from Apple and others.[7] Such a backdoor application can easily be exploited for illegal purposes by black hat hackers, for unjustified privacy infringement by other capable parties, and even for dictatorship by governments. Apple refused to comply with the request, and the court hearing was to take place in March 22, 2016. The FBI, however, withdrew the request saying that it found a way to hack into the phone in question without Apple's help. Now, Apple has to figure out what the vulnerability is in their iOS if it wants its encryption mechanism to be foolproof. Meanwhile, iOS users know that their data is no longer as secure as they once thought.

Around the same time, the Senate's draft bill, "Compliance with Court Orders Act of 2016," proposed that people should be required to comply with any authorized court order for data, and that if that data is "unintelligible"—meaning encrypted—then it must be decrypted for the court.[8] This bill is problematic because it practically nullifies the efficacy of any end-to-end encryption, which we use every day from our iPhones to messaging services like Whatsapp and Signal.

Because security is essential to privacy, it is ironic that certain cybersecurity measures are used to greatly invade privacy rather than protect it. Because we do not always fully understand how the technology actually works or how it can be exploited for both good and bad purposes, we need to be careful about giving blank permission to any party to access, collect, and use our private data without clear understanding, oversight, and consent. As we share more and more information online, cyberattacks will only increase, and organizations and the government will struggle even more to balance privacy concerns with security issues.

Why libraries should advocate for online privacy

The fact that people may no longer have privacy on the web should concern libraries. Historically, libraries have been strong advocates of intellectual freedom, striving to keep patron's data safe and protected from the unwanted eyes of the authorities. As librarians, we believe in people's right to read, think, and speak freely and privately as long as such an act itself does not pose harm to others. The Library Freedom Project is an example that reflects this belief held strongly within the library community.[9] It educates librarians and their local communities about surveillance threats, privacy rights and law, and privacy-protecting technology tools to help safeguard digital freedom. It also helped the Kilton Public Library in Lebanon, New Hampshire, become the first library to operate a Tor exit relay, to provide anonymity for patrons while they browse the Internet at the library.[10]

New technologies brought us the unprec-

edented convenience of collecting, storing, and sharing massive amount of sensitive data online. But the fact that such sensitive data can be easily exploited by falling into the wrong hands also created the unparalleled level of potential invasion of privacy. While the majority of librarians take a strong stance in favor of intellectual freedom and against censorship, it is often hard to discern a correct stance on online privacy, particularly when it is pitted against cybersecurity. Some even argue that those who have nothing to hide do not need their privacy at all.

However, privacy is not equivalent to hiding a wrongdoing. Nor do people keep certain things secrets because those things are necessarily illegal or unethical. Privacy allows us safe space to form our thoughts and consider our actions on our own without being subject to others' eyes and judgments. In his TED talk, Glenn Greenwald observes that even in the absence of actual massive surveillance, just the belief that one can be placed under surveillance at any moment is sufficient to trigger self-censorship and negatively affects one's thoughts, ideas, creativity, imagination, choices, and actions, making people more conformist and compliant.[11] This was further corroborated by the recent study from Oxford University, which provides empirical evidence that the mere existence of a surveillance state breeds fear and conformity and stifles free expression.[12]

Privacy is an essential part of being human, not some trivial condition that we can do without in the face of a greater concern. That's why many people under political dictatorship continue to choose death over life under mass surveillance and censorship in their fight for freedom and privacy. The Electronic Frontier Foundation states that privacy means respect for individuals' autonomy, anonymous speech, and the right to free association.[13]

We want to live as autonomous human beings free to speak our minds and think on our own. If part of a library's mission is to contribute to helping people to become such autonomous human beings through learning and sharing knowledge with one another without having to worry about being observed or censored, libraries should advocate for people's privacy both online and offline, as well as in all forms of communication technologies and devices.

Notes

1. This article has been revised from my previous blog post published on the ACRL TechConnect blog. Bohyun Kim, "Cybersecurity, Usability, Online Privacy, and Digital Surveillance," ACRL TechConnect Blog, May 9, 2016, http://acrl.ala.org/techconnect/post/cybersecurity-usability-online-privacy-and-digital-surveillance.

2. "SOC 2 and SOC 2 Type II Certification Defined," *NetGain Technologies,* http://www.netgainit.com/soc (accessed August 10, 2016).

3. Tolga Erbay, "Dropbox for Business Controls Audited: SOC 2 & SOC 3 Reports Now Available," Dropbox Business Blog, August 18, 2014, https://blogs.dropbox.com/business/2014/08/dropbox-soc3/.

4. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *The Guardian,* June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

5. Phil Matier and Andy Ross, "Cal Professors Fear UC Bosses Will Snoop on Them," *San Francisco Chronicle,* January 29, 2016, http://www.sfchronicle.com/bayarea/matier-ross/article/Cal-professors-fear-UC-bosses-will-snoop-on-them-6794646.php.

6. Scott Jaschik, "U of Big Brother?," *Inside Higher Ed,* February 1, 2016, https://www.insidehighered.com/news/2016/02/01/u-california-faculty-members-object-new-email-monitoring.

7. See Kim Zetter and Brian Barrnett, "Apple to FBI: You Can't Force Us to Hack the San Bernardino iPhone," *WIRED,* February 25, 2016, https://www.wired.com/2016/02/apple-brief-fbi-response-iphone/ and Shahid Buttar, "Apple, Americans, and Security

(continues on page 451)

explicit, and the project as a whole more pragmatic.

Our small group of instructors left the 360° Feedback Model project feeling that the experience was rejuvenating and increased our capacity as teachers. Although instructors were at times required to teach outside of our comfort zones, the process of collecting data from three data points, and immediately adapting in the classroom, ultimately built confidence that pedagogical change was both possible and, in fact, exciting. All instructors felt that they would be more likely to seek opportunities for pedagogical and professional development in the future.

Subsequent use of the model

Since the original iteration, the 360° Feedback Model has been used multiple times at our institution by small teaching cohorts. Each group has tweaked the process to its particular needs and timeframe, but the major elements of peer observation, student feedback, and self-reflection have remained constant. One cohort developed a peer observation instrument that asked observers to take notes on what the instructor and the students were doing at any given point throughout a lesson in order to ascertain how we and our students were engaging with each other and the lesson.

Conclusion: Bigger than the sum of its parts

The 360° Feedback Model leverages three modes of assessment in order to create something much more than simply three sets of instructional assessment data. In many cases, the process itself was as important as the feedback data. Comparing three sets of feedback often yielded insights more important than anything written in one feedback data set. Likewise, repeating observations allowed multiple chances for checking back in with colleagues as they implemented change in their classrooms. Repeating the instruction/observation process with the project's common curriculum made it very easy for observers to learn from colleagues and apply what was learned into his or her own classroom. Observing, teaching, reflecting, and adapting became a natural cycle by the end of the project, a cycle in which each instructor saw value and applicability to their own teaching practice.

("Cybersecurity and digital surveillance...," continues from page 445)

vs. FBI," Electronic Frontier Foundation, February 20, 2016, https://www.eff.org/deeplinks/2016/02/apple-americans-and-security-vs-fbi.

8. Andy Greenberg, "The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate,'" *WIRED,* April 8, 2016, https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/.

9. Library Freedom Project, https://libraryfreedomproject.org.

10. Library Freedom Project, "Tor Exit Relays in Libraries: A New LFP Project," https://libraryfreedomproject.org/torexitpilotphase1/ (accessed August 10, 2016).

11. Glenn Greenwald, "Why Privacy Matters," TED, October 2014, https://www.ted.com/talks/glenn_greenwald_why_privacy_matters.

12. See Jonathon W. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* 31, no. 1 (2016): 117–82, doi:10.15779/Z38SS13 (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645) and Glenn Greenwald, "New Study Shows Mass Surveillance Breeds Meekness, Fear and Self-Censorship," *The Intercept,* April 28, 2016, https://theintercept.com/2016/04/28/new-study-shows-mass-surveillance-breeds-meekness-fear-and-self-censorship/.

13. Electronic Frontier Foundation, "Privacy," https://www.eff.org/issues/privacy (accessed August 10, 2016).