ALA
Neal-Schuman
CHICAGO | 2019

ALA CENTER FOR THE FUTURE OF LIBRARIES

ANONYMITY

ALISON MACRINA AND TALYA COOPER

ALISON MACRINA is the founder and director of Library Freedom Project and a core contributor to The Tor Project. Her work aims to connect privacy and surveillance to larger struggles for justice. She has been awarded the Free Software Foundation's Award for Social Benefit and the New York Library Association's Intellectual Freedom Award, and she was a *Library Journal* Mover and Shaker.

TALYA COOPER is an archivist based in New York City. Previously, she was the digital archivist at the Intercept, where she managed the Snowden archive, and the archive manager at StoryCorps. She has written and presented about the intersections of archival ethics, privacy, and security.

ISBNs
978-0-8389-1633-9 (paper)
978-0-8389-1932-3 (PDF)
978-0-8389-1930-9 (ePub)
978-0-8389-1931-6 (Kindle)

Library of Congress Cataloging in Publication Control Number: 2019019623

Cover design by Kimberly Thornton. Composition by Alejandra Diaz in the Adobe Garamond Pro, Vista Sans and Vista Slab typefaces.

This paper meets the requirements of ANSI/NISO Z39.48-1992 (Permanence of Paper)

Printed in the United States of America
23 22 21 20 19 5 4 3 2 1

ALA Neal-Schuman purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

CONTENTS

FOREWORD

BY MIGUEL A. FIGUEROA

Center for the Future of Libraries
American Library Association

THERE'S A COMMON THROUGH LINE IN TODAY'S TECHNOlogical trends and developments that promise improved convenience and efficiencies: they trade on access to a broadening universe of public and private information and data.

An increase in surveillance systems (an estimated 245 million professionally installed video surveillance cameras were active and operational globally in 2014),[1] the movement toward "smart cities" (cities of all sizes are embarking on projects that will deploy technologies to collect and transmit information to improve city operations),[2] the ubiquity of voice recognition devices (the number of Amazon Echo installed bases in the U.S. grew to more than 30 million by 2017),[3] and other technology trends will ultimately exacerbate privacy concerns. As our concerns shift from the personal to the public, the resulting conversations may likewise swing from threats to privacy to the end of anonymity.

In *Anonymity,* Alison Macrina and Talya Cooper guide readers from privacy, a core value for our profession, toward a related appreciation and understanding for anonymity. They show how anonymity, the obscuring or withholding of identity, has implications for individuals, communities, and the libraries that serve them. While anonymity has that very real connection to our profession's fundamental value for privacy, the conversations library professionals must have regarding anonymity extend far beyond our users' experiences in or even with the library. Our communities exist in a world where lived experiences

1. https://technology.ihs.com/532501/245-million-video-surveillance-cameras-installed-globally-in-2014.
2. www.usmayors.org/wp-content/uploads/2018/06/2018-Smart-Cities-Report.pdf.
3. www.kleinerperkins.com/perspectives/internet-trends-report-2018.

in public and online have become a valuable source of data for governments, corporations, and other agents to collect and leverage.

Through "Understanding Anonymity," Alison and Talya help readers understand anonymity in our users' broader lives by providing an immersive vision for how anonymity plays out today and how it might continue to shift for the future. Their insight for how anonymity connects with library values centers the discussion in terms of both privacy and equity, recognizing that different users have varying needs for anonymity at distinct points in their lives.

From practical policies and procedures to technological interventions and educational instruction, "Anonymity in Libraries" shows how libraries can model anonymity's benefits and liabilities in a changing society. The Tor Project,[4] the LibraryBox Project,[5] and other initiatives show the promising directions that help ensure privacy while centering anonymity.

In "For the Future," Alison and Talya imagine new opportunities for libraries to advocate by standing up when policies or practices threaten individual rights to privacy and anonymity, educate by raising community awareness of the changing natures of privacy and anonymity, and implement spaces and technologies that make accommodations for anonymity while preserving security for staff and users alike.

It was Alison's work with the Tor Project and the Library Freedom Project that helped me better understand anonymity's significance for libraries. Here, with Talya, whose important advocacy in archives informs this work, they make clear why thinking about our futures requires thinking beyond the normal scope of our users' experiences in the library to also consider the library in the lives of our users. I continue to be inspired by leaders like Alison and Talya whose clarity of vision brings our traditions and values boldly into what may likely be a challenging future.

4. www.torproject.org.
5. http://librarybox.us.

UNDERSTANDING ANONYMITY

THE NEW NORMAL

YOU STEP OUTSIDE INTO THE BALMY SEPTEMBER evening, walk across the church parking lot, and open the door to your car with a sigh. Turning the red chip over as you hold it above the steering column, you think about the relativity of time. The past thirty days have been longer than any others you can remember, and it feels like actual years or even lifetimes have passed. You wouldn't have made it this far without the program and the ability it gives you to speak freely and openly among these strangers, protected by the practice of using only first names. You pop the coin into your wallet and pull out your smartphone, nonchalantly scrolling through Facebook, when something makes you pause over the "People You May Know" suggestions. Facebook has suggested that "You May Know" Bill R. and Mike M. from the meeting, except Facebook is telling you their full names, their family members, where they're employed, and all their likes. And it's telling them the same about you.

We live in an age of ubiquitous surveillance: many tiny pieces of our lives are constantly recorded, shared, and stored. We offer some of this information voluntarily in exchange for various services, while private corporations, law enforcement, and government intelligence agencies collect more of it almost invisibly. Libraries should be particularly concerned about the new norms of surveillance. Privacy has been one of the ALA's Core Values of Librarianship[1] since their adoption in 1939. Librarians have long recognized the relationship between privacy and intellectual freedom; when we lack privacy, we can't have intellectual freedom, because we are less likely to read, write, and research freely when we fear that we're being watched.

Privacy and anonymity are not synonymous, though. Privacy means that you get to control what information about you is shared. Anonymity, privacy's stricter cousin, means that in a given situation, no one knows your real identity. So why isn't this book about "privacy" rather than "anonymity," which sounds like something for secret agents and Internet trolls? Given the current surveillance environment, we believe that anonymity is as important for librarians to understand, support, and promote as privacy in general. Privacy has become a hot topic in libraries, with privacy-focused projects springing up all over the place—from the Data Privacy Project in New York City, to Library Freedom Project (of which one of this book's authors is founder and director), to the San Jose Public Library's Virtual Privacy Lab.[2] Anonymity, on the other hand, is still something of a curiosity for librarians—it is certainly present in the current fervor about privacy, but it is harder to understand and advocate for. We'd like to talk about why anonymity has value on its own, because of the ways that identity is weaponized

1. http://www.ala.org/advocacy/intfreedom/corevalues.
2. https://www.sjpl.org/privacy.

for surveillance purposes and monetized by big corporations. In order to understand why anonymity matters, it's important to know just what is happening to our data on the Internet these days.

PEOPLE YOU MAY KNOW

The opening story about Facebook identifying people who were anonymous to each other through its "People You May Know" tool is based on a real incident. Reporter Kashmir Hill heard innumerable anecdotes from users who'd found fellow patients of their psychiatrists and other attendees of support groups among their suggested friends, and reached out to Facebook to ask how and why the company was exposing these people to each other. Facebook admitted to using location services to "suggest friends."[3] After significant backlash, the company reversed course and denied that it had used location services as a factor in suggesting friends, finally admitting it had run "a small test to use city-level location to better rank existing [People You May Know] candidates."[4] In short, location services had been used to suggest friends at least for a portion of users for a period of time, which could have sufficed to de-anonymize a group of people in serious need of anonymity. Facebook also openly uses contact information (which it strongly suggests you upload upon creating an account) to chain users together. That function can be great if a user wants to get in touch with someone a mutual friend introduced them to at a networking event and that person appears as a "Person You May Know." But if two people have the same AA sponsor or mental health practitioner in their contacts and Facebook links them together and suggests that they "friend" each other, the "People You

3. https://splinternews.com/facebook-is-using-your-phones-location-to-suggest-new-f-1793857843.
4. https://splinternews.com/facebook-says-it-did-a-test-last-year-using-peoples-loc-1793857922.

May Know" feature starts to feel more like a gross violation of privacy, a nonconsensual disclosure of their identity.

This is not the only time Facebook has gotten in trouble for harmful or exploitative data practices. In 2018 alone, Facebook faced privacy scandal after privacy scandal,[5] and we can't point the finger at Facebook alone. The private companies that dominate the Internet collect huge amounts of data on users as part of their standard practice. The services we use for keeping up with friends, staying on top of the day's news, and for various modern conveniences like banking or shopping also track us elsewhere all over the Web, on our phones, and in the real-life spaces we inhabit. Big data is the business model, and there are few if any limits on how big these companies are able to get and how much information they're able to collect. Yet with so much precious information currency being generated, stored, and sold, data security seems like an afterthought. Major data breaches, from Equifax to Yahoo to the U.S. Office of Personnel Management, have spilled out the private details of hundreds of millions of people, and such breaches are all too commonplace.

All the data collected, stored, and often lost by private companies makes ubiquitous government surveillance easier than ever, coupled with the fact that law enforcement and intelligence agencies' surveillance budgets get larger and less transparent every year.[6] In 2013, Edward Snowden showed us how pervasive mass surveillance has become in the twenty-first century. We are subject to a byzantine network of entities that are capable of surveilling our every move and communicating it to each other, often in real time. The digital devices that have come to power our lives also generate a nearly invisible data trail that has proven

5. https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.
6. https://www.washingtonpost.com/wp-srv/special/national/black-budget/?noredirect=on.

highly valuable to all of those private entities. The combination of more data and better surveillance mechanisms means that the average computer user can expect that her most private information is in the hands of dozens of private companies and government apparatuses, regardless of who she is or what she's been doing. Those people whose data seems more interesting to law enforcement or intelligence agencies can expect even more surveillance, possibly with serious consequences.

To understand how all-encompassing this network is, let's imagine a person traveling from Los Angeles to Portland, Oregon. She wants to take her beloved St. Bernard, so instead of flying, she buckles in for a minimum fifteen-hour drive, during which she'll stop for a couple of meals and snacks, a whole lot of coffee, gas, and a number of rest stop breaks for the dog and herself. We all anticipate some level of surveillance, from a full-body scan to profiling in the TSA line, when we fly. But even this road trip will subject our two travelers to scrutiny by a vast number of public and private entities.

Leaving Los Angeles, this woman's car will be recorded by a number of cameras, some operated by law enforcement agencies and some operated by private companies: for instance, some repossession agencies use cameras and Automated License Plate Readers (ALPRs) to track car owners who are behind on their payments. Our traveler may also pay tolls with an electronic toll collection device, which records the time and location of the payment. This data could potentially be shared with a fusion center, a hub where federal agencies like the Department of Homeland Security and the Department of Justice collaborate with local, state-level, and tribal law enforcement. On her tiring drive, our traveler will pass no fewer than four fusion centers, from the Los Angeles Joint Regional Intelligence Center to the Oregon Titan Fusion Center in Salem. Local police also use ALPRs and compare the data they take

in to registries that attempt to match the plate number to crimes as serious as Amber Alerts and as banal as unpaid parking violations. As of 2011, 71 percent of police departments reported using this technology.[7] Moreover, we know that the traveler voluntarily exposes herself to all kinds of tracking through her cell phone's apps: the maps app she's using to find the quickest detours, the restaurant app that remembers her interest in vegetarian food, and the dating app she swipes idly while her dog sniffs around at the rest stop. The phone itself serves as a tracking device—it functions by sending electromagnetic signals to the closest cell tower, and law enforcement or a wireless carrier can easily find the location of the most recent cell tower a phone has "pinged."

These are just the technologies we know are in use, though. Let's say the traveler's license plate bears a similarity to the license plate number of a car that was used in a crime. Potentially, law enforcement at a fusion center could access the footage from a CCTV camera at a rest stop and use facial recognition—a technology that's advancing so rapidly it will soon be able to identify masked protesters[8]—to determine whether or not the traveler is the person they have in mind. Other technologies can pull in data about her and her trip through means that we don't even know about yet. And this is all before our traveler posts on Facebook about her trip, which will make the whole story openly available to law enforcement, third-party apps she's unwittingly allowed to access her posts, and anyone else who might be interested in her whereabouts.

7. https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/.
8. https://www.theverge.com/2017/9/6/16254476/facial-recognition-masks-diguises-ai.

How did we come to live in a terrifying sci-fi novel? Information has become a precious commodity that is fought over by major corporations, intelligence agencies, law enforcement, nation states, and hackers. Technology has permeated our lives by creating conveniences that would have seemed to belong to a far-distant future as recently as just ten years ago. As consumer devices have grown increasingly sophisticated, so have police surveillance capabilities. The regulatory environment has been wheezing to keep up as digital giants like Google and Amazon vacuum up smaller companies and expand their reach into our day-to-day lives, and intelligence agencies add zeroes to their enormous budgets. The future as seen by the master dystopian author Philip K. Dick is here. What does a digital resistance movement look like? And how can librarians take part in it?

We began by talking about how a private company can sabotage the much-needed anonymity of one of its users. While the potential for anonymity, and privacy in general, is deeply threatened by this *Black Mirror* episode of a future that we're now living in, librarians and libraries can play a pivotal role in allowing our communities to use the Internet without unregulated private companies and powerful government agencies learning who they are and what they're doing. When it comes to the Internet, anonymity is autonomy. As with other kinds of freedoms, people can abuse tools that grant them anonymity and free them from the consequences that voicing opinions and acting under their "real" identities might have. But anonymity also has the potential to make the Internet into a more democratic place, giving voice to the powerless rather than to the powerful.

The idea that anonymity can help someone safely and confidently express their beliefs long precedes the Internet. As librarian Chuck McAndrew of the Lebanon Public Library in New Hampshire points

out, "When I talk about anonymity with people, I like to point out that Thomas Paine published 'Common Sense' anonymously originally. That was one of the most influential books that spawned the American Revolution. From the start of this country, anonymity has had a very important point in the [democratic] process." Anonymous whistleblowers have played a key role in exposing abuses of power and miscarriages of justice. As an employee of the RAND Corporation in the late 1960s and early 1970s, Daniel Ellsberg began to believe that the United States' involvement in the Vietnam War was unjust, and so he anonymously leaked the "Pentagon Papers," a set of documents that showed the Johnson Administration had systematically deceived the American people about the war. His leaks were later published by the *New York Times*. These documents helped turn public opinion against the war and established a legal precedent for newspapers to publish leaked materials. Ellsberg's need for anonymity was situational and temporary; he turned himself in not long after leaking the papers to Neil Sheehan at the *New York Times*. But anonymity gave him the cover he needed to get the job done. A lower-stakes recent example is the beloved Italian author Elena Ferrante, who writes pseudonymously because, she says, she wishes "to liberate myself from the anxiety of notoriety and the urge to be a part of that circle of successful people."[9] When a journalist attempted to unmask her by trawling through tax and financial records, the literary world responded to his would-be expose with outrage and indignation,[10] questioning how revealing the identity of an author who so values her anonymity would add to readers' appreciation or understanding of her work. Similarly, many street artists operate anonymously in order to avoid prosecution for work

9. https://www.vanityfair.com/culture/2015/08/elena-ferrante-interview-the-story-of-the-lost-child-part-two.
10. https://www.npr.org/sections/thetwo-way/2016/10/03/496406869/for-literary-world-unmasking-elena-ferrantes-not-a-scoop-its-a-disgrace.

that, while technically illegal, has high value both for the communities where their art appears and, for some, in the art market.

In the past few years, archivists and oral historians who work with collections that represent marginalized and vulnerable communities have also thought through the value of anonymity for the people their collections represent. It can be difficult to strike a balance between ensuring that personal accounts and stories are preserved for the historical record and guaranteeing the safety of individuals who go on the record. During the 2015 Society of American Archivists annual conference in Cleveland, where a police officer had recently been acquitted of manslaughter after shooting two unarmed black people, a group of archivists recorded a set of oral histories. In the wake of the acquittal, the group wanted to create a collection—now known as the People's Archive of Police Violence in Cleveland[11]—to describe the grinding regularity of police violence and harassment that many people of color in Cleveland experience. The archivists understood that talking about experiences with the police could be challenging for many in the community: some people were involved in ongoing court cases, while others feared retaliation for speaking out against the police. Consequently, the archivists allowed many of their participants to record their stories anonymously, or to use only a first name or pseudonym. Historians tend to view anonymous accounts as less valuable to the record because they can't be verified. The creators of this archive acknowledge this critique in the online collection description by stating that "despite the anonymity, this collection will be useful for the larger and complex narratives of police violence in Cleveland that it conveys." In essence, they used anonymity as a way to tell a story both in individual voices and as an aggregated account, without putting anyone at risk.

11. http://www.archivingpoliceviolence.org/collections/show/2.

HOW DO YOU GET TO BE ANONYMOUS?

It's hard to be anonymous, though. In the early days of the Internet, many users embraced online identities divorced from their in-real-life (IRL) ones: think about AOL and GeoCities screen names like BookLover465 or BostonTerrierLuv. Since Facebook began to require that users provide a "real" first and last name and a valid phone number, and flags users who have not provided that information, it's become both technically difficult, and in some contexts, socially unacceptable, to be anonymous online. In 2010, Mark Zuckerberg famously told a journalist that "having two identities for yourself is an example of a lack of integrity."[12] Although Facebook softened its stance and does not require full names for some of its other products (Instagram, for instance), it suspends the accounts of users who have either been reported or algorithmically determined to be using fake names. Transgender rights activists, among others, have organized against this policy.[13] As people transition or explore their gender identities, they often choose to go by new names. They also may want to shield themselves from discovery by family members or colleagues who don't know about their new identity. Far from reflecting "a lack of integrity," these names can represent online identities that are truer to people's real selves than their state-assigned identities, in a space that allows them to express those identities safely.

A number of quasi-anonymous apps have seen brief swells in popularity, including the "gossip" apps YikYak and Whisper. It may be that in the post-Snowden era, more people in the mainstream are attracted to the idea of anonymity than ever before. People have come to realize

12. https://venturebeat.com/2010/07/21/live-blog-zuckerberg-and-david-kirkpatrick-on-the-facebook-effect/.
13. https://www.theguardian.com/world/2017/jun/29/facebook-real-name-trans-drag-queen-dottie-lux.

anonymity's power in a networked world, a power that some Internet users see fit to abuse. The infamous imageboards 4chan and 8chan require no registration and keep no memory, and have served as the breeding grounds[14] for pernicious movements like GamerGate, a 2014 campaign of harassment against women in the gaming industry so vicious that several of its targets went into hiding, fearing for their lives. These imageboards are also frequently credited with the rise of the "alt-right" and resurgent white supremacist movements in the United States.[15] These Internet movements use anonymity to create real-life chaos for people through the practice of "doxing"—finding, publishing, and using someone's personal information without their consent. In a heralded 2010 TED Talk, 4chan founder Chris "m00t" Poole described the imageboard's success in unmasking the identity of an animal abuser, to applause from the audience. We now tend to see this tactic as harmful, as doxing often represents an attempt to intimidate or silence activists or other politically outspoken people. Women, LGBTQ people, and people of color are much more likely to be targeted. Behind the shield of anonymity, malicious Internet users send threats of physical harm and employ tactics like "swatting" (calling in false reports of serious crimes so that a horde of law enforcement officers show up at a target's home or workplace) in an effort to intimidate them. In an interview published on NPR, Robin Nelson, a black feminist and biological anthropologist, expressed deeply mixed feelings about exposing her identity online:

> I am finding that this kind of conservative self-policing is not worth it—issues around black women's health and safety, personal safety and policing in black communities, issues of sexual harassment and assault more broadly have to be discussed by everyone, particularly

14. https://www.dailydot.com/layer8/8chan-pedophiles-child-porn-gamergate/.
15. https://www.theguardian.com/technology/2016/dec/01/gamergate-alt-right-hate-trump.

> by those who have any kind of inclination, privilege, or platform. Thus, while I am finding myself speaking out more about these issues—I know I do so with considerable risk to my career and perhaps my physical safety. I have been trolled on Twitter following tweets about sexism and sexual harassment in academe, and racist policing in black communities. I have genuine concerns about being doxxed.[16]

Using her own identity online allows Nelson to speak up for—and from the perspective of—several marginalized groups. At the same time, it makes her vulnerable to online harassment from anonymous Twitter trolls, many of whom tend to be white men, coming from a position of relative privilege.

But there are easily just as many examples of anonymity for good, some even using the same outlets as the bad. Many people know about the hacker collective Anonymous, a leaderless online movement that uses anonymity to perform "ops" or mass protest movements. They came to fame after Project Chanology,[17] an op directed at exposing the pernicious aspects of the Church of Scientology. They organized online, conducting DDoS (distributed denial of service) attacks to bring down Scientology websites, and also held in-person protests. A significant amount of this organizing happened on 4chan, the same anonymous imageboard where GamerGate and the alt-right developed.

Researchers and academic librarians reading this text may have heard of Sci-Hub, a database of academic papers created as a form of protest against the exorbitant fees that journals charge libraries and scholars for access. Its creator, Alexandra Elbakyan, founded the service in frustration

16. https://www.npr.org/sections/13.7/2015/02/26/389233371/a-toxic-stew-risks-to-women-of-public-feminism.
17. http://www.newsweek.com/anonymous-takes-scientology-93883.

when, as a student at an under-resourced university in Kazakhstan, she could not access the materials she needed for her work.[18] Today, the site has over 150 million papers. If a user requests an article that is not currently in Sci-Hub's database, the service uses a set of library credentials—donated by anonymous academics who support the site's mission to provide free access to information—to log into a library database and retrieve the file. Sci-Hub's success depends on a broad, anonymous community of people with a shared interest and belief in the freedom of information. Many librarians support Sci-Hub's guerrilla open-access work because they see libraries compelled to funnel increasing percentages of their budgets into expensive subscriptions for academic journals.

Many news organizations, like the Intercept, where one of the authors formerly worked, receive anonymous submissions of leaked materials through instances of the open-source platform SecureDrop (which is also made possible by Tor onion services). Whistleblowers have used this platform to send in materials that exposed covert government programs and corporate malfeasance. Revelations that came about from anonymous submissions to Secure Drop have led to public uproar, lawsuits, and legislative change. Subsequent government prosecution of several anonymous leakers reflects the serious threat that these whistleblowers face, and the strength of de-anonymizing technologies that the government has in its arsenal.

As these examples show, anonymity allows for more open sharing of information and for individuals to speak freely without fear of repercussions, abilities we consider key components of a democratic society.

18. https://www.washingtonpost.com/local/this-student-put-50-million-stolen-research-articles-online-and-theyre-free/2016/03/30/7714ffb4-eaf7-11e5-b0fd-073d5930a7b7_story.html?utm_term=.94566b422754.