

How has the fight for anonymity and privacy advanced since Snowden's whistle-blowing?

Media, Culture & Society

2019, Vol. 41(4) 565–571

© The Author(s) 2019

Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/0163443719843867

journals.sagepub.com/home/mcs**Gabriella Coleman** 

McGill University, Canada

Abstract

This article examines the legal, social, and political forces in a post-Snowden era that clarified the stakes around privacy and anonymity all while pulling more people into the orbit of a contemporary privacy and anonymity movement. It compares and contrasts the 100-year period in which US courts fleshed out free speech ideals and recent grass-roots privacy and anonymity initiatives that have come to reach a critical mass, highlighting the importance of civil society, journalists, and especially hackers whose aggressive pursuit of practical solutions have created the conditions for acting anonymously and securing privacy in our current era.

Keywords

anonymity, hacktivism, post-Snowden era, privacy

Today, thanks to the Internet, most people – not just traditional authors with access to publishers (Griffin, 1999) – have the ability to be, speak, and act anonymously. Whether its image boards, Internet chat rooms, ‘dark web’ marketplaces and communities, blogs, video games, mailing lists, or even some social media platforms like Twitter, scores of people can log onto these sites to write, speak, interact, and even act publicly without having to reveal one’s legal identity or location. In spite of these new-fangled possibilities for being anonymous or pseudonymous, the level of protection afforded by today’s technology is in fact only skin deep.

Anonymity online tends to be social in nature, with absolute technical anonymity much harder to achieve, though developments in software such as the Tor Browser have

Corresponding author:

Gabriella Coleman, McGill University, Montreal, QC H3A 0G4, Canada.

Email: enid.coleman@mcgill.ca

made this a more promising prospect. Moreover, everything we do online – whether at home or on a mobile device – is also being tracked, traced, compiled, crunched, bought, and sold by familiar tech-titans (Google, Facebook, and Verizon to name a few), and hundreds of lesser known data brokers who help advertisers build frighteningly detailed digital profiles of users by harvesting data from a variety of sources, including, but not limited to, customer databases and different online platforms (Christl, 2017; Zuboff, 2019). Both governments and corporations are in the business of surveillance, even if they offer varying justifications for their activities. Governments vacuum up reams of information about their citizens in the name of security, while corporations use similar methods for targeted advertising in the name of satisfying consumer needs and preferences. After I lecture to my students on this very topic, rattling off a dozen mechanisms by which corporations and governments can spy and pry on us, threatening both anonymity and privacy – distinct even if overlapping concepts – their reaction usually wavers between indifference (because they think they have nothing to hide) and, for those that I've convinced that caring is important, despair.

Indeed, I understand why so many of us get sucked into a hopeless vortex of doom and gloom when all the details about the scope, breadth, and depth of contemporary surveillance are laid bare. But if we also step back to consider the wide-ranging ethical, legal, and philosophical defenses now animating both the right to anonymity and privacy and the tools being developed to protect them, the situation might not be quite as dire as it first appears. Akin to the way that free speech ideals were both defined and fleshed out over a 100-year period as they pierced public consciousness during pitched political battles – such as those waged in Spokane by the Industrial Workers of the World in the early 1900s or by the Berkeley free speech protests in the 1960s (Stone, 2004) – so too have grass-roots privacy and anonymity initiatives reached a critical mass. For the first time in history, these issues have gravitational pull, clarifying the stakes around privacy and anonymity all the while pulling more citizens into the orbit of this nascent movement.

For the past 100 years, privacy, specifically, has been theorized in the liberal tradition as a right – ‘the right’, as Louis Brandeis and Samuel Warren (1890) famously put it in 1890, ‘to be let alone’ (p. 193). Developed in legal cases and statutes over the course of the 20th century, the right to privacy – the right to control what information is known about you or the ability to carve out zones of seclusion and refuge – has become a primary democratic concern. Anonymity, like privacy, also secures a zone of protection but it operates distinctly in so far it enables publicity of some sort – often speaking but also acting – as it renders the anonymous person unidentifiable and thus unreachable. While privacy is often lauded as a human right, anonymity receives far more critical scrutiny, if not downright condemnation, due to the fact that cloaking can provide cover for criminals and harassers, even as it allows for more noble quests such as truth telling. Theoretical and legal takes on anonymity – the right to act, speak, or associate in a group without having to reveal who you are – came a bit later. Taking into account the US context, only in the 1950s did Supreme Court cases and law journal articles in the United States begin to consider with far more depth and nuance the role of privacy and eventually anonymity in enabling democratic free speech (Schwartz, 1961; *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 1961). For instance, during the height of civil rights movement, the government Alabama sought to prevent the National Association for

the Advancement of Colored People (NAACP) from conducting business in the state through a legal injunction that demanded various documents from the NAACP including its membership lists. The Supreme Court deemed Alabama's disclosure demands unconstitutional, in violation of freedom of association, noting, in specific, 'Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs' (NAACP v. Patterson, 1958). Although the Supreme Court Justices tethered the issue of freedom of association to the question of privacy, legal scholars have argued that these and similar cases precipitated/preceded arguments around disclosure, anonymity, and political speech that would soon follow (Schwartz, 1961, p. 1903).

Not long after, in the early 1970s, a string of dramatic exposés leveled against the US government were also made possible by anonymous sources, and likely led to greater social awareness of anonymity with respect to truth telling. The Citizens Commission to Expose the FBI revealed massive secrets concerning Federal Bureau of Investigation (FBI) surveillance programs against protesters and dissenters (Medsker, 2014). Meanwhile, Deep Throat (i.e. Deputy Director Mark Felt) was the anonymous source who unveiled the Nixon Watergate scandal in 1972. While many revolutionary and oppressed groups have relied on secrecy to operate, not all of them have theorized anonymity in the way literary authors (Griffin, 1999), or as political groups, have done so in the past. A number of political movements founded in the 1980s and 1990s contemplated the role of anonymity in bringing attention to injustice. In North America, Guerrilla Girls, an artist and feminist ensemble founded in 1985, is one of the most famous collectives who have theorized cloaking as follows: 'Our anonymity keeps the focus on the issues, and away from who we might be' (Guerrilla Girls, 2018). Similarly, a Tunisian resistance network, Takriz (2009), highlights the role of anonymity in its tag line: 'Tunisian cyber think/fight tank & street resistance network since 1998. Free, True & Anonymous -Takrizo Ergo Sum- We make revolutions!'

By 1995, the US Supreme Court considered a case about the legality of distributing anonymous political material – *McIntyre v. Ohio* – and enshrined most clearly why anonymity is a necessary condition for free speech. Scores of civil libertarians can now cite any number of powerful quotes from the ruling: '[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication', wrote the court, 'is an aspect of the freedom of speech protected by the First Amendment' (*McIntyre v. Ohio Elections Commission*, 1995).

Yet, these events, legal cases, or groups made possible by the cover of anonymity and related debates and arguments in its support have tended to be punctuated and limited in reach until quite recently. In the last two decades, more citizens have experienced online anonymity, and particularly in the last 5 years, justifications and demands for privacy and anonymity have escaped the rarefied atmosphere of legal theory, policy making, and academic discourse and have additionally entered into the hands of technology collectives, journalists, radical librarians, filmmakers, hackers, software and hardware developers, and non-governmental organizations (NGOs) of varying stripes. More so, the right to privacy has been matched by a more sophisticated understanding of its relationship to anonymity as projects and writers have sought to pry apart these two values that are too often treated interchangeably (Nissenbaum, 1999).

In the context of growing certainty that government and corporate technologies have been effectively chilling, or otherwise pre-empting the meaningful exercise of both privacy and anonymity, a range of civil society organizations, journalists, and hackers have aggressively pursued practical solutions to problems concerning surveillance, which by extension have also created conditions for acting anonymously and securing your privacy.

The intelligence documents leaked by Edward Snowden were significant in this regard and for three different though interrelated reasons. First, and perhaps most obviously, the detailed reportage based on the documents furnished the public with a level of concrete details about the government's frighteningly robust capacities and capabilities for surveillance – and its willingness to illegally and legally exploit the corporate collection of data for its own ends – that simply did not exist before; among other revelations, we learned about the National Security Agency's (NSA) voice recognition capabilities (Kofman, 2018) and its XKeyscore program, which has amassed enormous amounts of social media, email, and Internet search traffic of ordinary people around the world in the name of national security (Granick, 2017; Weissman, 2015).

Unsurprisingly, these disclosures were experienced by many in the hacker community, which was already heavily invested in fighting for privacy and anonymity, as a historic and urgent wake-up call. New projects have sprung up in the form of encryption tool development and campaigns aimed at changing laws and social norms. Countless existing policies, technologies, and activist projects in the United States and the United Kingdom, initiated by groups such as the Electronic Frontier Foundation, Fight for the Future, Courage Foundation, the Open Technology Institute, Library Freedom Project, Big Brother Watch, and Privacy International, have found new foci and have further amplified their reach. Targeted grassroots policy and technological campaigns, such as Reset the Net (2014), seek 'to spread NSA-resistant privacy tools' so that they might become default features of the Internet – whether through their normative uptake or their outright encoding into basic technological protocols. Technologies like The Amnesic Incognito Live System (also known as Tails, an operating system built for anonymity), Tor (or The Onion Router, an open source project developing a popular anonymizer), Signal (an encrypted chat and phone application), LEAP (a recursive acronym for the LEAP Encryption Access Project, which modifies existing encryption tools to make them user-friendly), and SecureDrop ('an open source whistleblower submission system' now used by many journalism outfits) are being developed and deployed, and funded by private citizens and new media organizations like the Freedom of the Press Foundation. A stream of newer scandals, such as the revelations that Cambridge Analytica used personal data harvested from Facebook to influence election results, have amplified these concerns, and demonstrated the extent to which questions about personal data and privacy remain very much unsettled.

Finally, Edward Snowden – a well-known public figure already lionized in Hollywood and documentary films – has used his platform to educate scores of students and other members of the public through copious speaking engagements that cover everything from threats to privacy and anonymity to the practical steps citizens can take to stop them. I personally witnessed him speak at the university where I teach and the crowd he drew in was nothing short of astonishing. Although we only had 600 seats, thousands lined up for hours for a chance to see him, and when it was clear, most of them would not

get a chance to be seated, a riot nearly broke out (after we informed him of the dicey situation, he graciously agreed to live stream the event). Some students were likely only there because he was a well-known public figure, but he used his time judiciously to meaningfully educate the audience about civil liberties. Anyone who has seen his speeches knows just how passionately, but also cogently and reasonably, he defends the right to privacy and anonymity. His insights about privacy, surveillance, and anonymity like his now famous quip ‘Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say’ (Rusbridger et al., 2015) furnish the public with powerful aphorisms that distill complicated values in a mere sentence. If Mario Savio became the icon for the free speech movement of the 1960s, then Edward Snowden occupies a similar slot for the contemporary privacy and anonymity movement.

The global movement known as Anonymous obviously deserves mention. Unlike Edward Snowden, Anonymous, a protest movement that courted controversy, in no way commands the same sort of respect as he does, even in hacker, activist, and civil liberties circles. This is largely due to the prolific illegal acts taken under their name, including hacking and distribution of denial of service attacks. Still they have been the most visible collective acting and speaking under the mantle of anonymity and have dramatized the importance of anonymity and privacy in an era where both are rapidly eroding. Thousands of individuals across the globe from Mexico to Hong Kong have taken the name to experiment in the art of self-effacement, both insisting that one does not seek fame and recognition for contributing to righteous political causes, while using the shield of anonymity to bring attention to social grievances from police brutality to government corruption.

To be sure, just because there are more prominent figures, organizations, justifications, news outlets, collectives, and projects rallying citizens to fight for privacy and anonymity, and more hackers developing anonymity and privacy tools, does not mean that these efforts will dismantle, bypass, or monkey-wrench surveillance machines that erode and undermine these values. Given the existing state of most anonymity tools, attaining absolute technical anonymity is still currently unattainable – at least for most citizens. To thoroughly conceal your digital tracks, whether it be your location, behavior, habits, consumer preferences, and web searches, you have to take hefty, time-consuming measures. Many of us lack the time, knowledge, and patience to transform ourselves from traceable humans to untraceable ghosts.

Nevertheless, in the span of a mere decade, many of the existing tools have gone from almost unusable to usable – and more vitally have been placed in the hands of those who need it the most: dissidents, journalists, researchers, human rights workers, and public interest lawyers. Edward Snowden relied on a suite of these tools to communicate with journalists to leak material and documents. Today, a subclass of these tools – like Signal and the Tor Browser – are as easy to use as most other Internet apps or pieces of software. The tools themselves are designed with privacy and anonymity in mind and help inculcate those values as they spread and are adopted (Flanagan et al., 2008).

The existence of a social movement offers no guarantee of success, though of course this is a predicament faced by every single social movement, ranging from the environmental to civil rights endeavors. Those who measure the success of political movements in the weeks, months, or even years to come often rely on a neoliberal calculus,

expecting neat, tidy, and quick returns when the reality is that these sorts of battles are won quite slowly, with enormous effort, and over long periods of time. The fact that at the start of the new century there was barely a conversation about the problems with mass surveillance, while today we can start taking small steps to protect our data or be anonymous, is certainly not an occasion to blindly celebrate, as if the battle for privacy and anonymity has been won. It is simply an occasion to acknowledge that the battle has just begun.


Acknowledgements

I'd like to thank my research assistant Yuan Stevens for her research on the legal and political history of anonymity and her thoughtful comments for this piece.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Gabriella Coleman  <https://orcid.org/0000-0003-1679-8988>

References

- Brandeis L and Warren S (1890) The right to privacy. *Harvard Law Review* 15(5): 193–220.
- Christl W (2017) Corporate surveillance in everyday life. *Cracked Labs*. Available at: <http://crackedlabs.org/en/corporate-surveillance> (accessed 11 July 2018).
- Flanagan M, Howe D and Nissenbaum H (2008) Embodying values in technology: theory and practice. In: Van den Hoven J and Weckert J (eds) *Information Technology and Moral Philosophy*. Cambridge: Cambridge University Press, pp. 322–353.
- Granick J (2017) *American Spies: Modern Surveillance, Why You Should Care, and What to Do about It*. Cambridge: Cambridge University Press.
- Griffin R (1999) Anonymity and authorship. *New Literary History* 30(4): 877–895.
- Guerrilla Girls (2018) *Our Story*. Available at: <https://www.guerrillagirls.com/our-story> (accessed 4 April 2019).
- Kofman A (2018) Finding your voice: forget about Siri and Alexa – when it comes to voice identification, the ‘NSA reigns supreme’. *The Intercept*, 19 January. Available at: <https://theintercept.com/2018/01/19/voice-recognition-technology-nsa/> (accessed 11 July 2018).
- McIntyre v. Ohio Elections Commission (1995) 14 U.S. 334 (Supreme Court of the United States).
- Medsger B (2014) *The Burglary: The Discovery of J. Edgar Hoover's Secret FBI*. New York: Vintage Books.
- NAACP v. Patterson (1958) 57 U.S. 449 (Supreme Court of the United States).
- Nissenbaum H (1999) The meaning of anonymity in an information age. *The Information Society* 15(2): 141–144.
- Reset the Net (2014) Fight for the future. Available at: <https://www.resetthenet.org/> (accessed 30 January 2018).
- Rusbridger A, Gibson J and MacAskill E (2015) Edward Snowden: NSA reform in the US is only the beginning. *The Guardian*, 22 May. Available at: <https://www.theguardian.com/us-news/2015/may/22/edward-snowden-nsa-reform> (accessed 11 July 2018).
- Schwartz B (1961) The supreme court: October 1959 term. *Michigan Law Review* 59(3): 403–430.

- Stone G (2004) *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism*, 1st edn. New York: W.W. Norton.
- Takriz (2009) Tunisian cyber think/fight tank & street resistance network since 1998. Free, True & Anonymous -Takrizo Ergo Sum- We make revolutions! Available at: <https://twitter.com/takriz?lang=en>
- The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil (1961) The constitutional right to anonymity: free speech, disclosure and the devil. *The Yale Law Journal* 70(7): 1084–1128.
- Weissman CG (2015) It turns out the NSA was collecting voice calls, photos, passwords, documents, and much more. *Business Insider*, 1 July. Available at: <http://www.businessinsider.com/nsa-xkeycore-surveillance-program-details-revealed-in-new-snowden-documents-2015-7> (accessed 11 July 2018).
- Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Publicaffairs.