14 Understanding and Maintaining Your Privacy When Writing with Digital Technologies

Lindsey C. Kim

Overview

As our students utilize more networked technologies in their writing, it has become critical that both students and teachers understand the role privacy plays in their digital activity.* This chapter aims to help students understand why privacy is an important concept to consider when writing online and to provide them with the knowledge and strategies necessary to preserve their privacy in digital environments. First, it will offer an explanation of information privacy based on three central concepts: data, agency, and flow. After explaining each of these concepts in detail, it will then turn to a discussion of how students can leverage this knowledge to exert more control over the information they share when composing online.

Before beginning this chapter, I walked into my office at home and shut the door. Had I not done this, writing this chapter would have been quite difficult. Closing my door prevented the variety of interruptions that might disrupt my ability to write, like my young daughter's tendency to find me and demand I sing along with her to her favorite song, or the vibrant conversation that echoes from a family member's Zoom meeting, or even the sound of some breaking development from a news clip on the family television. Closing the door allowed me to create a *private* space, a space where I could focus on my writing relatively

undisturbed. Privacy, in many ways, shapes our writing and our writing processes. Virginia Woolf, in her famous extended essay, *A Room of One's Own*, emphasizes this very connection between privacy and writing. To quote her famous thesis, a woman must have "a room of her own if she is to write" (4). That is, if we want to engage in writing that creates new ideas, arguments, and fictions, privacy is one thing that we need.

Woolf's claim that pairs writing so significantly to privacy was first published in 1929, but it has renewed relevance today, when advances in digital technologies have caused massive reconsideration of what the term "privacy" even means. The digital spaces that we find in our devices or online do not have the same walls as Woolf's room, so it can be difficult to understand precisely what role privacy as a concept plays in digital writing. In order to do so, we have to consider a different way of thinking about privacy: information privacy. This chapter aims to help you understand why the privacy of your personal information and data matters to your online activities. First, it will explain what information privacy is, noting the similarities and differences of information privacy compared to the more common space-based ways of understanding privacy (like Woolf's room or my office). It will present a way of understanding and analyzing information privacy based on three central concepts: data, agency, and flow. After explaining each of these concepts in detail, the chapter will then turn to how you can use these concepts to become more informed about the privacy of your information when using digital products or services, as well as how you can leverage such knowledge to protect your privacy online.

What Is Information Privacy?

When we think of privacy, we most likely think of it in terms of physical space. Certainly Woolf does when she argues for the necessity of a *room* of one's own. When I walk into my bedroom or office and I close the door and shut out potential intrusions or interruptions, I have, to echo Woolf, a space of my own. We can refer to this type of privacy as *spatial privacy*. This way of thinking of privacy is firmly fixed in the way many of us experience the world. I can see or touch physical material, such as land, wood, or concrete, so it is easy to conceptualize and create structures to keep others out, like walls or fences. This notion of privacy is also heavily embedded in U.S. society. Take, for instance, the concept of private property, where people can own land and deny others access to that land. Many U.S. American laws depend on spatial notions of privacy, such as the Sixth Amendment, which protects our homes from "unreasonable searches and

seizures" ("The Bill of Rights," Art. VI). In this way of thinking, a space is private when we are one of a few people (if not the only person) who has access to it. Our private spaces are ones we have control over—we can decide who has access to them and who does not.

We can certainly see echoes of this way of thinking about privacy in our digital spaces. In many ways, our devices have become our digital homes, to which we seek to limit access with security systems and passcodes. Yet this way of understanding privacy is often incompatible with networked activity (or activity that occurs any time you use a device or service that connects to the web). For starters, networked activity requires near constant connection between users, platforms, services, and devices, so the concept of basing privacy purely on limiting access to our devices just does not work. In other words, when we do stuff online, we invite a lot of people and entities to access our devices, and this connection and exchange of information is the driving force of networked activity, thus our understanding of privacy in digital spaces must shift to account for this increased degree of access and interaction. Additionally, digital, rather than physical, infrastructures require us to understand privacy in a new way, because what we are protecting access to is fundamentally different. Instead of being made of dirt, wood, or brick, our digital spaces are composed by code and information. Since our writing, work, and personal activities are happening in networked digital spaces just as much as in physical ones, we need a way of thinking about privacy that addresses this fundamental difference and can offer us better guidance for writing and acting in digital spaces. *Information privacy*, then, switches our focus from spaces to the information that composes digital activity.

Data

Each interaction with a networked technology leaves a trace of your actions in the form of information. John Cheney-Lippold, an expert in digital studies, demonstrates the sheer volume of information that is produced from a single, simple networked action:

> A simple web search from even the most unsophisticated of smart phones generates a lengthy record of new data. This includes your initial search term, the location of your phone, the time and day when you searched, what terms you searched for before/after, your phone's operating system, your phone's IP address, and even what apps you installed on your phone. Add onto this list everything

> else you do with that phone, everything else you do on your computer, everything else that might be recorded about your life by surveilling agents. (4)

These traces of information can be intentional, like when I like a picture or write a tweet. We knowingly produce and put this information out into the web (though we are not always fully aware who will see it). However, oftentimes, we unintentionally or unknowingly create informational traces. For instance, every time I click or visit a website, that visit is recorded, along with a lot of other data about that interaction, such as how long I visited the page, the type of device I am using, my location, etc. This data-about-data is called *metadata* and is the most invisible of the data that we produce online. Often, we pay little attention to our intentional traces of information, and even less to our unintentional ones. However, such data, or the bits and pieces of information we produce through interactions and activities online, are very important because they help to shape the digital environments that we write within.

The data that you produce online is used by companies and platforms to personalize your user experience, from your Google search results, to the products you see on Amazon, to your Netflix queue. Personalization is largely the product of the interpretation of your personal data by *algorithms*. In a sense, these algorithms act as filters, letting through the information they deem appropriate based on your activity and personal information, while blocking out the rest. This highly personalized web of information is what digital activist Eli Pariser calls a "filter bubble" (9). He describes the filter bubble as "your own personal, unique universe of information that you live in online," and it depends on the information gathered about you by the various companies behind the filters (9). Simply put, the information that companies gather about you through your digital activity plays a large role in determining the information and content that you see while on the web.

Your personal information does more than just shape what *you* see online, however. Jessica Reyman, a scholar who studies digital rhetoric and writing, argues that our information helps compose online spaces, services, and platforms. She writes, "With every click and path followed, every status update and tweet entered, every photo and post contributed, every comment, every item tagged, users are collectively producing both the visible and invisible social Web" (514). In other words, through our digital activities we all write the web, at least in a sense. This is important because not only do we influence our digital tools and spaces, but they influence us. I write very differently with a pencil than with a word processor or with

a speech-to-text device. In each of these scenarios, the technology writes *with* me. It is not a unidirectional relationship where I tell the word processor exactly what to write and such is done. In many ways, the word processor itself pushes back, exerting influence on the writing I am producing. An example of this influence is through the grammar and spell checking mechanisms embedded in a word processor. The different-colored squiggly lines exert influence over how I compose, whether it be the red line that compels me to correct my spelling of unidirectional when, in my hasty typing, I accidentally transposed two letters, or the blue line earlier in the document that informed me of my "long sentence" that I should "consider revising." The word processor also impacts my design of this document, as I can only format the text or structure the text in ways that it allows me to. To put it differently, I have agency over these networked technologies, but these technologies also influence me and constrain my agency in certain ways. Given the significance of data to networked activity as well as the significance of digital technologies to our writing and other everyday activities, agency over these aspects thus becomes an incredibly important element of thinking through digital privacy.

Agency

Agency, at its simplest, is the ability to produce an effect through your actions. If you have agency, you are able to exert at least some influence on the happenings around you. In the opening example, I exerted agency over the privacy of my space by closing the door and reducing access to my office. In the context of information privacy, we can think of agency as the ability to affect the collection and use of your personal information, both that which is intentionally and unintentionally produced. Unfortunately, in many instances where we use the web, our agency tends to be limited in both these regards. This lack of agency is due in large part to the fact that we tend to give up control over our data, either knowingly or unknowingly, when we write online. Reyman writes that "when users access, read, network, post, or compose within many online spaces, they are simultaneously giving up information about a wide range of their online activities and, ultimately, giving up control and ownership of their contributions" (514).

Allowing the corporations behind our digital products, services, and platforms such unfettered access to and complete control over the information we produce via our digital activity can cause a variety of problems, especially for your writing. For instance, let's return briefly to the filter bubble concept. If our search queries only return biased results, then we

aren't able to engage in effective argument or discussion. It is hard to engage in any type of dialogue over civic or personal issues when everyone is working from different information. One person could be working with government data, and another could be working from a conspiracy theory. Moreover, filter bubbles can easily become echo chambers, places where we *only* experience content that reaffirms our thoughts and perspectives. As Pariser writes, "By definition, a world constructed from the familiar is a world in which there's nothing to learn. If personalization is too acute, it could prevent us from coming into contact with the mind-blowing, preconception-shattering experiences and ideas that change how we think about the world and ourselves" (15). Personalized information flows like this can be a problem precisely because we have little agency in the matter. We have little to no say in what makes it through the filter (or not). Pariser shares a story of the frustration he experienced when he realized the consequences of this limited agency. Because of his liberal political leanings, he tended to interact more with his progressive or liberal friends' posts on Facebook. Facebook's algorithm prioritized engagement, so his conservative friends began disappearing from his feed. This greatly upset Pariser, who always made it a point to try and interact with different perspectives. But what troubled Pariser most was the fact that he never realized it was happening until it was too late. His data was being used in a way he never consented to, one that actively went against his goals and values, and barring quitting Facebook altogether, there was nothing he could do to change it.

Let's return to Woolf's *A Room of One's Own*, the piece that started our discussion. An (or perhaps *the*) essential message of that piece is that women need private spaces to write because those private spaces grant women relief from the pressure (and pain) of oppressive social and cultural systems. Woolf shares a story about how, when she was visiting a prestigious university that only men could attend, she wandered into a patch of grass, and was immediately accosted by a security guard who harshly instructed her to return to the paths, as women were not permitted off of them. Her identity as a woman, and the biases and prejudices directed toward that identity, resulted in her actions being policed. Much like our physical spaces, our digital spaces too are full of these types of oppressions and biases largely due to the fact that our data is used to ascribe us certain digital identity categories. Cheney-Lippold starts his book on data and identity, "In a database far, far away, you have been assigned a gender, ethnicity, class, age, education level, and potentially the status of parent with x number of children" (3). While this may initially seem harmless, it can be extremely problematic. In 2011, Safia Noble, a researcher and profes-

sional in digital communications, discovered how racism and sexism can be embedded in the algorithms of Google's search function. When looking for some content for her young nieces, she recounts how simply searching for the terms "black girls" resulted in pages of graphic pornography (3). An essential part of the privacy of Woolf's room of her own is that it allows writers to be spared the pressures of social norms and harms of social oppressions. Thus, having the ability to enact agency over our data, to restrict access to it, not only allows us to exert control over the digital spaces we inhabit, but also allows us to distance ourselves from digital structures that may be reproducing and imposing the same harmful prejudices that exist offline.

Flow

To complete our understanding of information privacy, we have to understand how our personal information moves and where it goes. In other words, we have to understand how it flows. Helen Nissenbaum advocates a conception of privacy based on appropriate information flow. According to this way of thinking, information must be shared and is intended to be shared, but the data subjects (or the people who the data is about) have a right to expect it will be shared appropriately. But what does it mean to share something appropriately? Well, according to Nissenbaum, what's appropriate is determined by the situation. To examine a situation to determine what is appropriate flow (and what is not), we can build on the framework that Nissenbaum establishes by asking the following questions about an exchange of information (in physical, textual, or digital contexts):

- What context surrounds the information? What are the norms and structures that govern that context?
- What actors are involved in the situation? That is, who is sharing the information, who is receiving it, and who is the information about?
- What type of information is being shared?
- How might we characterize the sharing that is happening? Is the sharing happening as a gift? An economic exchange? An obligation?
- Are there any rules or constraints regarding how the information is shared?

Consider, for a moment, your educational information (such as your grades, course schedule, etc.). Information describing your educational ac-

tions and history flows within a university *context*. Your educational information flows between various *actors* in these contexts, from professors, to advisors, to registrars, to administrators, and more. Any of these actors can send or receive information about students (who would be the information subject in this instance). It would be inappropriate for your educational information to flow to actors outside the university context. You would not want, say, your dentist, an actor outside the university context, to have access to your educational history. The *type* of information also plays a role in determining if the flow of the information is appropriate or not. Information about your GPA might be more appropriate for some actors, while information about your course schedule might be better suited for others. Because of the way the education system functions, teachers are generally obligated to share grades with students, because otherwise how would students know if they are indeed learning the material and passing the course? Obligation, here, then *characterizes* the type of sharing that's occurring. Finally, FERPA is a law that governs how your educational information is shared. For instance, if you are over 18, there are special forms that must be filled out before instructors can share information regarding your grades with your parents. This law acts as a *constraint* on how the information can be shared (or not).

In digital spaces, where information flow is evitable, Nissenbaum presents a more contextualized version of privacy that proves to be quite useful, especially for analyzing the near constant flow of our information in digital environments. For instance, you might deem it appropriate to give a platform access to your data to help improve your user experience, but find it incredibly invasive and inappropriate for them to share that data with a third party for advertising purposes.

Another aspect of information flow to consider when writing or engaging in any sort of networked activity is the content that flows to you. Many digital spaces and products are designed around attention and engagement, and because of this, many digital products constantly vie for users' attention through a variety of mechanisms, from amplifying sensational or appealing content, as in the case of Pariser's Facebook feed, or via constant notifications. Consider the fact that almost every application you install on your phone asks for one of two things (and often asks for both): access to your information and the ability to send you notifications. Such constant notifications are problematic for writing, as noted in the introduction, as they can easily and quickly become interruptions that divert our attention from our writing. Thus, considering the flow of information and content to you as well as the degree of control you have over that flow

is an important factor in engaging in writing in online spaces (or engaging in any other sort of productive activity online). As demonstrated by my opening example, an essential component of privacy involves the ability to shut out interruptions or intrusions, which we can do through critical consideration of the content and information that flows into our own digital networks and devices.

Maintaining Your Privacy Online

We've discussed three important elements of information privacy and how each relates both to writing with digital technologies and other networked activity. In this final section, we will shift from an examination of information privacy itself to discussing ways to preserve your privacy as you write and act in networked spaces. We will discuss two major aspects of exercising more control over the information you share online: 1) gaining knowledge about a technology or platform's data gathering practices, and 2) using this information to exert the most amount of control over your personal information possible in your writing practices.

First, for technology or platforms that you use often or that gather sensitive data information, you should work to gain a greater understanding of their data practices. You will want to try to discover *what* data is being gathered, *how* it is used, and with *whom* it is shared. Oftentimes, these details can be difficult to research, since the answers can be spread across different texts, obscured through difficult language, or kept hidden via confidentiality or copyright laws, but it is still important to investigate such things to the extent that you can, especially for the technologies that you use regularly. For instance, terms of service agreements or privacy policies often provide a lot of information regarding corporations' data practices. For products that collect a lot of data, you can often find more detailed data use policies, though these documents can be even more technical and difficult to read than terms of service agreements or privacy policies. While these documents can provide general information on companies' data practices, such policies are insufficient in and of themselves, as they only contain information on general practices and can often be written in difficult or inaccessible ways. Plus, there is often a degree of bias with such documents—they are drafted by companies that own and operate the digital service, so there is an increased risk that such documents will obscure or downplay potentially off-putting information. As such, it is always a smart move to triangulate such sources with other sources. A great resource to compare such documents against is ToSDR.org, which stands for "Terms

of Service; Didn't Read" ("Frontpage"). It is an online service where users summarize and rate the policies outlined in terms of service agreements, and offers a glimpse at the digital service's policies from a critical perspective that centers users' needs.

After researching the data gathering practices of different technologies, you can exert agency over the privacy of your data through critical consideration of the digital technologies you use in your writing or other digital activity. There are other online tools you can use to help learn more about a service's data practices, tools that not only inform you but assist you in resisting such data gathering tactics. Ghostery is a browser extension that detects and blocks "thousands of third-party data-tracking technologies – putting control of their own data back into consumers' hands" ("About Ghostery"). Mozilla, the popular web browser, is an internet browser founded on the principles of transparency and open-access, and they have demonstrated a value for users' privacy. They write that "we believe that privacy is fundamental to a healthy internet" and promise to limit their gathering of your personal information only to the data that "serves you in the end" ("Firefox Privacy Notice"). The browser enacts these values by blocking thousands of common web trackers and by offering robust privacy controls so that you can customize what information you want to be available to whom. As mentioned before, this increased level of control and agency is another aspect you want to be on the lookout for when you are determining which devices and services you would like to be a part of your writing process. To gain a better understanding of the degree of control or agency a digital service, platform, or device offers you, examine the default privacy settings of the page. This page also usually offers good information about the flow of data about you as well as the flow of content to you. Services or technologies that are transparent and that offer users more agency in the ways their personal information is shared or in the degree of notifications sent to them are great indicators that those services and technologies can be trusted. Ultimately, these efforts help reduce the information that corporations have about you and your digital activity, which makes it more difficult for them to categorize you, personalize your experience, or intrude upon your digital activity.

Conclusion

If we were to revise Woolf's famous claim to reflect our digital age based on the information presented in this chapter, we might say something like this: People must be able to exercise some control over the flow of their

personal information and data to write with digital technologies. While a statement like this does not speak to all of the complexity of privacy in digital spaces, it does help you start to consider and analyze the role privacy plays in your digital writing and activities. By considering what degree of agency you wield regarding the flow of your personal information and data, you are fostering a more critical orientation toward your own relationship to technology, and both your writing (and personal activities) will benefit from it.

It is important to note that while it is good to develop critical orientations toward the technologies you write with and to gain greater understanding of information privacy, the scope of the issue goes beyond the actions of any individual user, as is common with any sort of complex problem. In other words, the burden of addressing issues of data and information privacy online should not be yours alone. It is simply not feasible. For instance, just reading the privacy policies for every service you use would take you 76 workdays per year, according to a study from 2008 (Reyman 521). Thus, the final, and perhaps most important way to help protect and preserve the privacy of your personal information and data in digital spaces is to advocate for it. However, politics and policymaking tend to be slow businesses, so in the meantime, you can look to the knowledge and skills provided in this chapter to help you out.

Works Cited

"About Ghostery." *Ghostery*, https://www.ghostery.com/about-ghostery/. Accessed 25 Aug. 2020.

"The Bill of Rights: A Transcription." *National Archives,* https://www.archives.gov/founding-docs/bill-of-rights-transcript. Accessed 28 Mar. 2021.

Cheney-Lippold, John. *We Are Data: Algorithms and the Making of Our Digital Selves*. NYU Press, 2017.

"Firefox Privacy Notice." *Mozilla*, https://www.mozilla.org/en-US/privacy/firefox/. Accessed 25 Aug. 2020.

"Frontpage." *Terms of Service; Didn't Read*, https://tosdr.org/. Accessed 28 Mar. 2021.

"Google Ad Settings." *Google*, www.google.com/settings/u/0/ads. Accessed 28 Mar. 2021.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford UP, 2010.

Noble, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York UP, 2018.

Pariser, Eli. *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press, 2011.

Reyman, Jessica. "User Data on the Social Web: Authorship, Agency, and Appropriation." *College English*, vol. 75, no. 5, 2013, pp. 513–33.

Woolf, Virginia. *A Room of One's Own*. Harcourt, 1981.

Teacher Resources for Understanding and Maintaining Your Privacy When Writing with Digital Technologies

This chapter aims to introduce students to the concept of information privacy, explain its impact on students' writing, and provide students with knowledge and strategies for regaining control over the information they produce on the Web. Such an essay would complement lessons on digital writing, research, and on critical digital literacies. Networks play a major part in our students' writing practices and in their digital habits, so this chapter can help students gain greater critical awareness of the role that their data plays in forming the web, as well as how it affects their writing. Moreover, it provides vocabulary to understand information privacy and its impact on their writing. This chapter focuses particularly on information privacy as it relates to corporate data-mining practices. It does not offer discussion on other issues that could regulate digital privacy more broadly, such as online harassment or doxxing. Some of the concepts and vocabulary can be applicable to such kinds of privacy invasions, and while the piece at times can gesture broadly to these types of intrusions, its focus remains primarily on data and data-mining since these practices are often less visible to students. Ultimately, these materials (both the chapter and these accompanying resources) aim to help students develop critical orientations toward the digital technologies and services that they integrate into their writing networks and processes.

Here are several discussion questions and in-class activities that can help students practice critically analyzing the data and privacy practices of the technologies they use or that can give them experience in exercising agency in regard to how their personal information is shared when they write online.

Discussion Questions

1. This chapter supplied you with some questions to help you analyze and determine the appropriate flow of information in a given context. Describe a time when you felt your privacy was breached due to inappropriate information flow. Using the questions from the chapter as a guide, explain why the instance was a breach of your privacy. How did the flow go wrong?

2. Current debates regarding privacy and data often involve the data-mining practices of popular social media companies. Pick a popular social media platform, and explain what you consider to be the appropriate flow of your personal information when using that platform. Describe the context of social media, which actors should be involved in the exchange of your personal information, what type(s) of information should be shared, what type of sharing you expect to occur, and whether there are any pertinent rules or norms that shape or constrain how your information is shared.

3. As mentioned in the conclusion to this chapter, while this chapter outlines ways of understanding and maintaining the privacy of your personal information online, there is only so much that one individual can do. Advocacy thus becomes a central part of preserving and shaping digital privacy. What kinds of policies and practices do you think should be implemented to help protect and preserve the privacy of your data and personal information online?

4. The chapter discussed the importance of integrating digital technologies and services that valued privacy, transparency, and offered you more control over the data you produce through your digital activity. Map out your writing "network" for academic writing, including the various digital devices, services, and platforms that you commonly use when writing a research paper for class. Are there any you might want to investigate further in regard to their data practices? Are there items you might rethink or revise after reading this chapter? Why or why not?

Exercises and Activities

Profiling and Revising Privacy Defaults

Pick a popular social media platform, preferably one that you already use, and investigate its default settings for privacy and for sharing information. Consider the implications for these defaults. What kind of information is shared and with whom is it shared? Is any potentially sensitive information shared with any problematic parties? Finally, what kind of revisions would you suggest to the defaults? Create a short presentation that summarizes the default settings, the potential implications of these defaults, and explains how you would revise the defaults so that users have greater control over their personal information and the data they produce.

Analyzing Terms of Service Agreements

Terms of service agreements, privacy policies, and data-use policies are great sites to begin to analyze the privacy practices of a digital service or platform. Yet, they are notoriously hard to understand due to everything from their difficult language and syntax to their length, so few users read them, causing their contents to remain unknown to many. "Terms of Service; Didn't Read" (ToS;DR) is a digital service that summarizes the content of these documents into short bulleted lists that are written in simple language ("Frontpage"). The short summaries also include ratings of the terms according to their fairness to users. Visit the website and review some of the entries. Then locate the entry for a platform or service that you either use or have used. Read both the terms of service agreement for the platform or service as well as the ToS;DR entry. Do you think that the entry accurately represented the terms? Is there anything you would change or include in the entry? For your final task, propose some revisions to the terms of service agreements that would make them more fair to users.

Investigating Your Digital Identity

If you have a Google account, visit your Google Ad settings at www.google.com/settings/u/0/ads to learn more about the data that Google has collected on your activities. How has Google categorized your interests and identity based on its algorithm's interpretation of your data? Do you think their profile presents an accurate picture of you? Why or why not?