

nior, who says she has “always slept with her phone,” comments, “Every channel, every day, the news is dominated by catastrophe.”

The students in the circle of fourteen expand on this: As they see it, the media supports a view of the world as a series of emergencies that we can take on, one by one. Events that have a long social and political history are presented as special, unusual, “unthinkable” events: massive oil spills, gun violence against elementary school children and their teachers, extreme weather—for the most part, all are represented as catastrophes. You know you are thinking in terms of catastrophe if your attention is riveted on the short term. In catastrophe culture, everyone feels part of a state of emergency but our agitation is channeled to donating money and affiliating with a website.

When you have an emergency, problems are there to be dealt with on an ad hoc basis. Even problems that involve global climate change or disregard for critical infrastructure are covered by the media as disasters that need disaster relief. You turn something that has a politics and a pattern into something that needs an immediate response but not necessarily an analysis. A catastrophe doesn't seem to require legislation. It needs balm and prayers.

To the circle of fourteen, life in a catastrophe culture suggests that you cope through connecting. Faced with a situation that you experience as an emergency, you want to use social media to huddle with your friends.

A twenty-three-year-old who was in middle school during 9/11 says, “Most of the emergencies that are broadcast on the media, you can't do anything about. There's no action you know how to take that would improve the actual circumstances.” This does much to explain how the fretful self navigates the media stream of bad news: We learn about something, get anxious, and connect online.

Catastrophes have the ring of an act of God. They happen to us and we can't see them coming. When terrorism is presented as a calamity, and it is, it is presented as separate from the history that created it, so that it comes to be more like a natural disaster, a state of evil, rather than something that can be addressed by politics or through a reconsideration

of its historical roots. When terror is treated as a natural disaster, all we can do about it is kill terrorists.

When you name something a catastrophe, there is nothing much to say. If you confront a situation that you see as shaped by human actions, there is plenty to say. You are in a position to demand accountability. You need to understand causes. You are considering action. You need to have a conversation. Many.

It is easier to face an emergency than to have those difficult conversations. When we go into crisis mode, we give ourselves permission to defer the kinds of conversations that politics requires. And right now, our politics requires conversations, too long deferred, about being a self and a citizen in the world of big data.

Room to Think in a World of Big Data

On our new data landscape, conversations that we traditionally have thought of as private—talking on the phone, sending email and texts—are actually shared with corporations that claim ownership over our data because they have provided us with the tools to communicate. Wherever we let our gaze fall online, we leave a trace that is now someone else's data. Insofar as we soul-search when we search the web and let our minds wander as we wonder what to read, what to buy, what ideas intrigue us, these introspective activities, too, belong to the company that facilitates our search. It mines them for data it finds useful now and saves them for what it might find useful in the future. For all of this information exists independently of us and is in a state, in parts and slices, to be sold to third parties. And outside this world of commercial transactions, we've learned that our government, too, feels that it has a claim on listening in.

Over time, living with an electronic shadow begins to feel so natural that it seems to disappear. Mark Zuckerberg, founder and CEO of Facebook, has said, “Privacy is no longer a relevant social norm.” Well, pri-

vacy may not be convenient for the social network, but what is intimacy without privacy? What is democracy without privacy? Is there free thought without privacy?

The World Without Privacy

My grandparents knew how to talk about this. At length. When I was ten, and my grandmother thought I was old enough to understand, she took me to the main public library in Brooklyn, a great, imposing structure at Grand Army Plaza. I already had a library card that I used at our local library, a few minutes' walk from our home. But now we were going to the big library.

My grandmother made a picnic lunch—chicken sandwiches on rye bread and lemonade—and we sat on the concrete-and-wood benches of the Prospect Park parade grounds. The conversation turned to the library “rules.” My grandmother wanted me to understand that I could take out any book. But the books I chose would be a secret between me and the library. No one had a right to know the list of books I read. It was like the privacy of our mailbox. Both protected what I would call *mindspace*. It was crucial to why she was so glad to be raising her family in America.

My grandmother had explained to me that in the Europe of her parents, the government used the mail to spy on people. Here, it was a protected space. (Clearly, my grandmother was less than informed about the excesses of J. Edgar Hoover, but she had taken comfort from the demise of Senator Joseph McCarthy.) We had talked about the privacy of mailboxes from when I was very young; indeed, as I remember it, the morning ritual of going down to get the mail gave my grandmother a new chance—almost every day—to comment on the reassuring mailboxes.

But the secrecy of my book list was something we didn't talk about until later. She clearly saw it as a more subtle civics lesson: how to explain to a child that no one should ever be able to hold what I read against me. Indeed, no one had the right to know what I was reading.

My grandmother's reverence for the American mailbox and library

was her deepest expression of patriotism. And mindspace was central to that patriotism. From my grandparents' perspective, as second-generation Americans in the Brooklyn working class, being able to think and communicate in private meant that you could disagree with your employer and make a private decision about whether you were going to join a union. When making this decision, you would be wise to read union literature in private. Otherwise you might be threatened or fired before you got to your decision. And you needed time to let your ideas jell. You needed privacy to change your mind about important matters.

During the televised confirmation hearings for Supreme Court justice Clarence Thomas, the question came up as to whether Anita Hill's testimony against Thomas would be supported if it could be shown that he was a regular viewer of pornography. Did he regularly check pornography out from his local video store? Hill's lawyers wanted those records to be entered as testimony. I believed Anita Hill; I wanted those video records to support her account of Thomas's vulgarity and harassment. But his advocates argued that video store records and the list of the books one withdraws from a public library should get the same protection. Clarence Thomas had a right to his mindspace. He won that round and I considered it a round that my grandmother would have wanted him to win.

We make our technologies and they make and shape us. I learned to be an American citizen at the mailboxes in an apartment lobby in Brooklyn. And my understanding of the mindspace that democracy requires was shaped by how things worked at the public library. I did not know where to take my daughter, now twenty-four, as she grew up with the Internet.

She had to learn that her email is not protected. And although her library books are still private, what she reads online is not. She shows me how she tries to protect her privacy—for example, on social media apps, she never uses her real name but rather multiple other names, a protective habit of a generation that learned to avoid predators on Facebook by not using real names. But she knows that anyone sophisticated and determined would be able to find her. And when it comes to her cell phone, she gives up all privacy for convenience. She wants to use maps, so the

GPS on her phone is turned on. This means that her phone leaves a trail of bread crumbs detailing her location. And the system knows her friends, what she searches for, what she reads.

When she was eighteen, my daughter showed me a program called Loopt. Like Find My Friends, it uses the GPS capability of the iPhone to show the location of friends. She thought it seemed creepy but told me that it would be hard to keep it off her phone if all her friends had it. "They would think I had something to hide."

And just recently, because I learned it just recently, I had to tell her that if she tries to protect her privacy by using browser settings designed to hide her identity, it may well activate greater surveillance of her online behavior. These days, the desire for privacy is considered suspicious and limits your ability to have it. This is distressing when I think of the lessons I learned at the public library. Wasn't the need for private mind-space why we protected the library books in the first place?

A generation grows up assuming nothing is private and offering faint resistance. Only a few years ago, a sixteen-year-old tried to reassure me that it somehow didn't matter that her email wasn't private by saying, "Who would care about my little life?" It was not an empowering mantra. And she turned out to be wrong. A lot of people care about her "little life."

Surveillance Creates the Digital Double

When the Internet was new, we thought of it as a frontier. Historian of technology Evgeny Morozov points out that the advertising tagline for Microsoft's Internet Explorer was "Where do you want to go today?" These days, our online practices put us in a world where the real question is "What do you have to *give* today?" What information about yourself will you offer up today? We exist alongside digital representations of ourselves—digital doubles—that are useful to different parties at different times, or for some, at a time to be determined. The digital self is archived forever.

Gradually, we have come to learn all of this. And in the post-Snowden years, we have learned more—that the calls, locations, and online searches of ordinary Americans are monitored. But almost everything about this process remains as secret as possible, shrouded under the mantle of national security or the claim of proprietary interests. Exactly what is taken? In what form? How long is it kept? What is it used for? What most people have come to understand is that this is out of their hands.

What happens to conversation in these circumstances? One thing I've already noted is that people tend to forget their circumstances. This is one of the great paradoxes of digital conversation: It feels private despite the fact that you are onstage. If you are on Gmail, your email is searched for clues for how to best sell to you, but for the individual, the experience of being on email remains intimate. You face a glowing screen and you feel alone. The experience of digital communication is out of sync with its reality. Online, you are under a kind of surveillance.

The Self of Self-Surveillance

Previously, when we thought about surveillance, we thought about the effects of being watched all the time. The English philosopher Jeremy Bentham had a model for it. He called it the panopticon. It is a way to construct a building: You put a guard at the hub of a spoked wheel. Since those who are living in the spokes don't know when the guard is looking at them, they act as if he always is, because he always could be. They put themselves on good behavior, conforming to what they think of as the norm.

It works for prisons; it works for asylums. The French sociologist Michel Foucault took Bentham's image of panopticon surveillance and made it relevant to thinking about being a citizen of the modern state. For Foucault, the task of the modern state is to reduce its need for surveillance by creating a citizenry that is always watching itself. With cameras on most corners, you don't misbehave even if you don't know if a camera is on any particular corner. It might be. This is the self of self-

surveillance. And it operates on the digital landscape. If you know that your texts and email are not private, you watch out for what you write. You internalize the censor.

Now, participation in the life of the data-gathering web has given “self-surveillance” a new twist. We do more than actively give up information by reporting our preferences or by taking surveys or by filling out forms. *These days, the most important data to those who watch us are the data trails we leave as we go about the business of our daily lives.* We feed databases as we shop, chat, watch movies, and make travel plans. Tracking one’s fitness, keeping in touch with friends on social media, using a smartphone—all of these make surveillance and social participation seem like the same thing. Every new service on our smartphone, every new app, potentially offers up a new “species” of data to our online representation. The goal for those who make the apps is to link surveillance with the feeling that we are cared for. If our apps take “care” of us, we are not focused on what they take from us.

In the world as Foucault analyzed it, when you put cameras on street corners, you want people to notice them and build a self that takes surveillance as a given. Knowing that the cameras are there makes you “be good” all by yourself. But in our new data regime, the goal is for everyone to be unaware, or at least to forget in the moment, that surveillance exists. The regime works best if people feel free to “be themselves.” That way they can provide “natural data” to the system.

So these days, while I might have only a general sense of where I’ve spent my day shopping, my iPhone knows, and this means that Apple knows and Google knows—a development I was not thinking about when I was thrilled to discover that, with GPS, my phone could double as an interactive map and I would never have to get lost again.

Shaped by the System: Living in the Bubble

Each of us who “feeds” the system ends up being shaped by it, but in a very different way than the person caught in the panopticon. We don’t so much conform because we fear the consequences of being caught out in deviant behavior; rather, we conform because what is shown to us online is shaped by our past interests. The system presents us with what it believes we will buy or read or vote for. It places us in a particular world that constrains our sense of what is out there and what is possible.

For any query, search engines curate results based on what they know about you, including your location and what kind of computer you are using. So, if you do a search about the Ukraine and opposition movements don’t come up, this may be because an algorithm has decided that you don’t want to see them. This means that you won’t learn (at least not then) that they exist. Or, by the logic of the algorithm, you may be presented with only certain political advertisements. You may not learn that a candidate who seems “moderate” in national advertising sends anti-gun control advertising to other people, just not to you.

The web promises to make our world bigger. But as it works now, it also narrows our exposure to ideas. We can end up in a bubble in which we hear only the ideas we already know. Or already like. The philosopher Allan Bloom has suggested the cost: “Freedom of the mind requires not only, or not even especially, the absence of legal constraints but the presence of alternative thoughts. The most successful tyranny is not the one that uses force to assure uniformity, but the one that removes awareness of other possibilities.”

Once you have a glimmer—and you only need a glimmer—of how this works, you have reason to believe that what the web shows you is a reflection of what you have shown it. So, if anti-abortion advertisements appear on your social media newsfeed, you may well ask what you did to put them there. What did you search or write or read? Little by little, as new things show up on the screen, you watch passively while the web actively constructs its version of you.

Karl Marx described how a simple wooden table, once turned into a commodity, danced to its own ghostlike tune. Marx's table, transcendent, "not only stands with its feet on the ground . . . it stands on its head, and evolves out of its wooden brain, grotesque ideas far more wonderful than 'table-turning' ever was." These days, it is our digital double that dances with a life of its own.

Advertising companies use it to build more targeted marketing campaigns. Insurance companies use it to apportion health benefits. From time to time, we are startled to get a view of who the algorithms that work over our data think we are. Technology writer Sara Watson describes such a moment. One day, Watson receives an invitation, a targeted advertisement, to participate in a study of anorexia in a Boston-area hospital. Watson says, "Ads *seem* trivial. But when they start to question whether I'm eating enough, a line has been crossed."

Watson finds the request to participate in the anorexia study personal and assaultive, because she is stuck with the idea that she made the invitation appear. But how? Is the study targeting women with small grocery bills? Women who buy diet supplements? We are talking through machines to algorithms whose rules we don't understand.

For Watson, what is most disorienting is that she doesn't understand how the algorithm reached its conclusion about her. And how can she challenge a black box? For the algorithms that build up your digital double are written across many different platforms. There is no place where you can "fix" your double. There is no place to make it conform more exactly to how you want to be represented. Watson ends up confused: "It's hard to tell whether the algorithm doesn't know us at all, or if it actually knows us better than we know ourselves." Does the black box know something she doesn't?

In conversations with others over a lifetime, you get to see yourself as others see you. You get to "meet yourself" in new ways. You get to object on the spot if somebody doesn't "get you." Now we are offered a new experience: *We are asked to see ourselves as the collection of things we are told we should want, as the collection of things we are told should interest us.* Is this a tidier version of identity?

Building narratives about oneself takes time, and you never know if they are done or if they are correct. It is easier to see yourself in the mirror of the machine. You have mail.

Thinking in Public

Thoreau went to Walden to try to think his own thoughts, to remove himself from living "too thickly"—how he referred to the constant chatter around him in society. These days, we live more "thickly" than Thoreau could ever have imagined, bombarded by the opinions, preferences, and "likes" of others. With the new sensibility of "I share, therefore I am," many are drawn to the premise that thinking together makes for better thinking.

Facebook's Zuckerberg thinks that thinking is a realm where together is always better. If you share what you are thinking and reading and watching, you will be richer for it. He says that he would always "rather go to a movie with [his] friends" because then they can share their experience and opinions. And if his friends can't be there physically, he can still have a richer experience of the movie through online sharing. Neil Richards, a lawyer, cross-examines this idea. Always sharing with friends has a cost.

It means we'll always choose the movie they'd choose and won't choose the movie we want to see if they'd make fun of it. . . . If we're always with our friends, we're never alone, and we never get to explore ideas for ourselves. Of course, the stakes go beyond movies and extend to reading, to web-surfing, and even thinking.

And even thinking. Especially thinking. One student, who was used to blogging as a regular part of her academic program for her master's degree, changed styles when she changed universities and began her doctoral studies. In her new academic program blogging was discouraged. She comments that, looking back, the pressure to continually publish led

to her thinking of herself as a brand. She wanted everything she wrote to conform to her confirmed identity. And blogging encouraged her to write about what she could write about best. It discouraged risk taking. Now, writing privately, she feels more curious. Research shows that people who use social media are less willing to share their opinions if they think their followers and friends might disagree with them. People need private space to develop their ideas.

Generations of Americans took as self-evident the idea that private space was essential to democratic life. My grandmother had a civics lesson ready when she talked about the privacy of my library books. In order to be open to the widest range of ideas, I had to feel protected when making my reading choices. "Crowdsourcing" your reading preferences, says Richards, drives you "to conformity and the mainstream by social pressures."

Objects-Not-to-Think-With

Cognitive science has taught us the several qualities that make it easy not to think about something you probably don't want to think about anyway. You don't know when it is going to "happen." You don't know exactly what it means for it to "happen." And there is no *immediate* cause and effect between actions you might take and consequences related to the problem.

So, for example, if you don't want to think about climate change, you are able to exploit the psychological distance between a family vacation in an SUV and danger to the planet. A similar sense of distance makes it easy to defer thinking about the hazards of "reading in public," the risks of living with a digital double, and threats to privacy on the digital landscape.

Here is Lana, a recent college graduate, thinking aloud about how she *doesn't think* about online privacy:

Cookies? I think that companies make it hard to understand what they are really doing. Even calling them cookies seems pretty brilliant. It

makes it sound cute, like it's nothing. Just helpful to you. Sweet. And it is helpful to get better ads or better services for the things you want. But how do they work and what are they going to do with all that they know about you? I don't know and I don't like where this is going. But I'm not going to think about this until something really bad happens concretely.

Lana is uneasy that data are being collected about her, but she's decided that right now she's not going to worry about it. She says that when she was younger she was "creeped out" by Facebook having so much information about her, but now she deals with her distrust of Facebook by keeping her posts light, mostly about parties and social logistics. She doesn't want what she puts on Facebook "coming back to haunt me."

More than this, Lana says, she "is glad not to have anything controversial on my mind, because I can't think of any online place where it would be safe to have controversial conversations." And she would want to have any conversation online because that is where she is in touch with all her friends. Lana describes a circle that encourages silence: If she had controversial opinions she would express them online, so it's good that she has none, because what she would say would not be private in this medium. In fact, Lana's circle has one more reinforcing turn: She says it's good that she has nothing controversial to say because she would be saying it online and everything you say online is kept forever. And that is something she doesn't like at all.

I talk to Lana shortly after her graduation from college in June 2014. In the news are manifestations of disruptive climate change, escalating wars and terrorism, the limitations of the international response to the Ebola epidemic, and significant violence due to racial tensions. There is no lack of things to communicate about "controversially." Yet this very brilliant young woman, beginning a job in finance, is relieved not to have strong opinions on any of this because her medium for expressing them would be online and there is no way to talk "safely" there.

But Lana does not say that she finds any of this a problem. It would be inconvenient to label it that way. If you say something is a problem,

that suggests you should be thinking about changing it and Lana is not sure that this is the direction she wants to take her feelings of discontent, at least not now. Right now, as for many others, her line is that “we all are willing to trade off privacy for convenience.”

She treats this trade-off as arithmetic—as if, once it’s calculated, it doesn’t need to be revisited.

Vague on the Details

When I talk to young people, I learn that they are expert at keeping “local” privacy—privacy from each other when they want to keep things within their clique, privacy from parents or teachers who might be monitoring their online accounts; here they use code words, a blizzard of acronyms. But as for how to think about private mindspace on the net, most haven’t thought much about it and don’t seem to want to. They, like the larger society, are, for the most part, willing to defer thinking about this. We are all helped in this by staying vague on the details.

And the few details we know seem illogical or like half-truths. It is illegal to tap a phone, but it is not illegal to store a search. We are told that our searches are “anonymized,” but then, experts tell us that this is not true. Large corporations take our data, which seems to be legal, and the government also wants our data—things such as what we search, whom we text, what we text, whom we call, what we buy.

And it’s hard to even learn the rules. I am on the board of the Electronic Freedom Foundation, devoted to privacy rights in digital culture. But it was only in spring 2014 that an email circulated to board members that described how easy it is to provoke the government to put you on a list of those whose email and searches are “fully tracked.” For example, you will get on that list if, from outside the United States, you try to use TOR, a method of browsing anonymously online. The same article explained that from within the United States, you will also activate “full

tracking” if you try to use alternatives to standard operating systems—for example, if you go to the Linux home page. It would appear that the Linux forum has been declared an “extremist” site.

One of my graduate research assistants has been on that forum because she needed to use annotation software that ran only on Linux. When she reads the communiqué about Linux and full tracking, she is taken aback, but what she says is, “Theoretically I’m angry but I’m not having an emotional response.” According to the source we both read, undisputed by the NSA, the content of her email and searches is surveilled. But still, she says, “Who knows what that means. Is it a person? Is it an algorithm? Is it tracking me by my name or my IP address?”

Confused by the details, she doesn’t demand further details. Vague understandings support her sense that looking into this more closely can wait. So does the idea that she will be blocked or perhaps singled out for further surveillance if she tries to get more clarity.

One college senior tells me, with some satisfaction, that he has found a way around some of his concerns about online privacy. His strategy: He uses the “incognito” setting on his web browser. I decide that I’ll do the same. I change the settings on my computer and go to bed thinking I have surely taken a step in the right direction. But what step have I taken? I learn that with an “incognito” setting I can protect my computer from recording my search history (so that family members, for example, can’t check it), but I haven’t slowed down Google or anyone else who might want access to it. And there is the irony that articles on how to protect your privacy online often recommend using TOR, but the NSA considers TOR users suspect and deserving of extra surveillance.

I come to understand that part of what sustains apathy is that people think they are being tracked by algorithms whose power will be checked by humans with good sense if the system finds anything that might actually get them into trouble. But we are in trouble together. Interest in Linux as probable cause for surveillance? We’re starting not to take ourselves seriously.

My research assistant says she’s not worried about her data trail be-

cause she sees the government as benign. They're interested in terrorists, not in her. But I persist. Now that my assistant knows she is subject to tracking because of her activity on the Linux forum, will it have a chilling effect on what she says online? Her answer is no, that she will say what she thinks and fight any attempt to use her thoughts against her "if it should ever come to that." But historically, the moments when "it came to that" have usually been moments when it has been hard or too late to take action.

I recall how Lana summed up her thoughts about online privacy: She said she would worry about it "if something bad happens." But we can turn this around and say that something bad *has* happened. We are challenged to draw the line, sometimes delicate, between "personalization" that seems banal (you buy shoes, so you see ads for shoes) and curation that poses larger questions.

In the 2012 presidential election, Facebook looked at random precincts and got people to go to the polls by telling them that their friends had voted. This political intervention was framed as a study, with the following research question: Can social media affect voter turnout? It can. Internet and law expert Jonathan Zittrain has called the manipulation of votes by social media "digital gerrymandering." It is an unregulated threat. Facebook also did a study, a mood experiment, in which some people were shown posts from happy friends and some people were shown posts from unhappy friends to see if this changed their moods. It did. Social media has the power to shape our political actions and emotional lives. We're accustomed to media manipulation—advertising has always tried to do this. But having unprecedented kinds of information about us—from what medications we take to what time we go to bed—allows for unprecedented interventions and intrusions. What is at stake is a sense of a self in control of itself. And a citizenry that can think for itself.

Snowden Changes the Game

I have been talking to high school and college students about online privacy for decades. For years, when young people saw the "results" of online data collection, chiefly through the advertisements that appeared on their screens, it was hard for them to see the problem. The fact that a desirable sneaker or the perfect dress popped up didn't seem like a big deal. But in the years since Edward Snowden's revelations about how the government tracks our data, young people are more able to talk about the problems of data mining, in some measure because it has become associated (at least in their minds) with something easier to think about: spying. What Snowden was talking about seemed enough like old-fashioned spying that it gave people a way into a conversation about the more elusive thing: the incursions of everyday tracking.

So, after the Snowden revelations, high school students would begin a conversation about Snowden and then pivot to "Facebook knowing too much." What did Facebook know? What did Facebook keep? And had they really given it permission to do all this?

Or they would begin a conversation by talking about how they were trying to stay away from Facebook, now a symbol of too much online data collection, and then pivot to Snowden. A different set of issues entirely, but Snowden gave them a handle on their general sense of worry. The worry, in essence: How much does the Internet "know" and what is the Internet going to do about it? After Snowden, the helpful ads on their screens had more of a backstory. Someone, many someones, knows a lot more about them than their sneaker preferences.

And yet it is easy for this conversation to slip away from us. Because just as we start to have it, we become infatuated with a new app that asks us to reveal more of ourselves: We could report our moods to see if there are concerns to address. We could track our resting heart rate or the amount of exercise we get each week. So we offer up data to improve ourselves and postpone the conversation about what happens to the data we share. If someday the fact that we were not careful about our diet in