that was inevitable, with responsibility lying with celebrity-obsessed media organizations and not Snowden himself). But they also showed that one can play the instruments of celebrity, surveillance, virality, and visibility for personal, even noble gain. His relative success was far from assured. An array of forces, from administration-friendly media outlets to senators calling Snowden a traitor, soon coalesced to counter the former NSA contractor's media campaign. There also was no guarantee that the public might not eventually turn against Snowden. As soon as he became a public name and face, a horde of journalists, well-wishers, security officials, and others began tracking Snowden's every move, swarming Hong Kong hotels and, later, the Moscow airport. As any Hollywood star might claim and any paparazzo might confirm, it's exceedingly difficult to embrace some parts of fame while evading others. Managing visibility is a full-time job, and Snowden's reputation will continue to be litigated in the court of public opinion, perhaps for years.

from Jacob Silverman, TERMS OF SERVICE (2015)

# The War Against Identity

**Anonymity is a shield from the tyranny of the majority . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.**

**—Majority opinion in Supreme Court case *McIntyre v. Ohio Elections Commission***

Whether you take your cues from postmodernism (it's all a performance) or your parents (you can be anything you want, dear), most of us are made to think that identity is mutable. Your identity can change, sometimes as easily as buying new clothes or finding a new watering hole, with people who know you not as a banker but as the guy who likes to go bowling and drink old-fashioneds on Friday nights. Many of us experience this sense of possibility most poignantly at the beginning of college, that much prophesied transition that's supposed to be all about starting over, becoming the person you couldn't be in high school.

In the social-media age, all of this is changing—perhaps irrevocably—and particularly for the college set. Arrive on campus now and all of your new friends will be able to pore over your Facebook profile, ingesting the CliffsNotes version of your teens. For many, this

is an uncomfortable realization. The clinical psychologist and technology researcher Sherry Turkle says that "this sense of the Facebook identity as something that follows you all your life is something that many adolescents feel is a burden." Identities are no longer toyed with, tried on and cast off, adopted for various settings or as a method of exploration. No, they're cloud-based, filtered through a standardized profile that never forgets. As Turkle says, "Now there's one identity that counts—it's the Facebook identity." It must be carefully tended to and managed, because it's the only one you have.

The relative decline of Facebook usage among young people may be attributed, at least in part, to this growing feeling of stasis. (The influx of older Facebook users, who render the network uncool and easily monitored by parents and other authority figures, also doesn't help.) Private and ephemeral messaging apps such as Snapchat, Kik, and WhatsApp offer young people—who are already used to cleverly managing their privacy when dealing with prying parents at home—an opportunity to communicate creatively with less fear of repercussion. Like e-mail, these apps aren't immune to eavesdropping, but they help return communication to a more protected space. Messaging apps are, however, illusory in the measure of privacy they offer. Just as Google did with Gmail—scanning private e-mails to serve up ads and contribute to the records the company holds for each user—there is little reason to think that messaging companies won't submit to similar tactics. Surveillance and advertising remain the industry-standard business models. And though Facebook, which purchased WhatsApp in a $19 billion deal, has promised to respect that company's privacy-friendly policies, it's hard to believe that one of the world's biggest data-mining firms won't make some use of all the juicy consumer information passing through its networks.

This is the problem when communication becomes inextricable from surveillance, data permanence, and publicity. From a social networking profile to one's Google search results, one's identity is increasingly a matter of public consumption. In some sense, each of us is now a public



figure, thanks to the development of digital systems designed to make sure that Internet users are always locatable and identifiable by their real names, all so that they can be connected to a digital profile that reflects their tastes and habits. When these systems are combined with smartphone GPS data and the proliferation of advertising screens, sensors, cameras, and facial recognition throughout our urban environments, we are looking at a future where we will never be anonymous, even when walking down the street. The local barista may not remember your face or your order, but the sensor in the coffee shop's doorframe will, and it'll tell him to get started on that double espresso as soon as you pass by it with your smartphone. Advertisements will follow you throughout your day, using billboard cameras to recognize your face or a sensor in a bus stop to identify your phone. Once you submit and buy the new video game they're pushing, they'll harness your social graph and move on to your friends, imploring them, "Jacob bought this game this morning. Don't you want to play with him?" Based on their demographic data, your friends may be offered a higher price, but they won't know that.

This scenario raises some uncomfortable questions. What does it mean to be anonymous, beyond the ability to say something without attaching our names to it? Are we on the path to trading the freedom and flexibility of anonymity for the conformity of the named? Who really benefits from making social-media users employ real names and fixed, stable identities? Is it online communities, or is it the managers of social networks, the ad purveyors, the data brokers, and the intelligence agencies? Is anonymity a right worth fighting for, or has it been ruined by a host of bad actors?

## TELL US YOUR REAL NAME

Google's Eric Schmidt has cast himself as a philosopher-king of digital networking, assuring us that he has a clear eye of where these technologies are headed and how his company can avoid crossing the "creepy"

line. He also has a tendency to sound somewhat detached from the very societal transformations his company is helping to foment. Consider some of his comments about the changing nature of online identity.

"For citizens, coming online comes to mean living with multiple identities; your online identity becomes your real identity," Schmidt once said. "The absence of a delete button on the Internet will be a big challenge. Not just what you say and write, but also the Web sites you visit, and do or say or share online. For anyone in the public eye, they will have to account for their past."

In the same interview, Schmidt raised concerns about online behavior, explaining that parents will have to talk to their kids about what he called "digital footprints" as much as they will about sex. Some parents, he speculated, may give their kids unusual or, alternatively, common names, depending on how they want them to show up in Internet search results—essentially practicing search-engine optimization, known in industry circles as SEO, from birth. (A few years earlier, Schmidt said that perhaps young people, in order to shed their digital trails, should be given the right to change their names upon turning eighteen. Of course, people already have that right.) He said that fake digital identities, complete with concocted records of online shopping, may become equally valuable to dissidents and drug dealers.

Schmidt was mostly speculating, riffing on recent history and trying to predict where we might soon be headed. His remarks carry some truth and his predictions seem possible, but what is stranger about it all is how removed Schmidt sounds from the very concerns he's presenting. This is, after all, one of the most powerful people in the technology industry, the executive chairman of Google, a company that has done as much as any other to push for the use of fixed online identities and established widespread Internet surveillance, and he's apparently concerned about the consequences of these same practices. If only someone could tell Eric Schmidt this! He might actually do something about it.

Demonstrating a shift in rhetoric, if not in practice, Facebook has been far more paternalistic in telling us why we must always be identifiable online. It is apparently for our own good. In an interview with Charlie Rose, Sheryl Sandberg, the company's COO, said, "The social Web can't exist until you are your real self online. I have to be me, you have to be Charlie Rose." Here is the airy rhetoric of authenticity, though what represents a "real self"? If I use the Tor software—favored by activists, hackers, and cyber-criminals alike to anonymize their Web browsing—am I being inauthentic? If I change my Facebook name so that an ex can't find me, am I being insincere? Company founder Mark Zuckerberg went so far as to impugn his users' character, explaining: "Having two identities for yourself is an example of a lack of integrity." His sister Randi apparently agrees. In July 2011, Randi Zuckerberg, who at the time was Facebook's marketing director, said: "I think anonymity on the Internet has to go away." She claimed that "People behave a lot better when they have their real names down."



Regulating behavior is an odd goal for a company devoted to connecting people. Such a policy can easily lead to measures to chip away at users' freedom of expression or to coerce them into certain actions. (Facebook's history of secret experimentation on users, along with its interest in boosting ad click-through rates, suggests that they are already deeply involved in the behavior modification business.) And there's little evidence that these sorts of real-name policies accomplish much. In the last decade, South Korea experimented with requiring real names to post comments on many Web sites, eventually requiring them on all sites that received more than 100,000 visitors per year. But so-called malicious comments only decreased by less than 1 percent, while people who posted frequent harsh comments appeared undeterred.

The more important question is not whether these policies work to reduce rudeness or antisocial behavior (the definition of which may vary widely not only between cultures but also among individuals), but whether companies should be allowed to impose such requirements on users. The U.S. Postal Service, for example, doesn't require you to use your legal name to mail a letter; why should digital media be any different? While many companies claim to worry about civility online, they in

fact have financial incentives in establishing real names for their users. A user who is always browsing and posting under her real name is easier to track, monetize, and keep within certain bounds of approved behavior. And with U.S. social-media firms directly tied to the country's surveillance programs, your complete digital dossier is potentially available to the U.S. government. Seen this way, anonymity becomes closely linked to privacy, to control over who knows your identity and when they're allowed to know it. An assault on anonymity is an assault on privacy.

Facebook's anti-anonymity rhetoric is wrongheaded; it's also hypocritical. In May 2011, a report surfaced explaining that Facebook employed a public relations firm to urge journalists to air privacy concerns about Social Circle, a Google search feature that allows users to see search results that draw on their friends' social-media feeds. The PR firm, Burson-Marsteller, didn't reveal who its client was, but the relationship was exposed by a journalist for the *Daily Beast*. This type of mudslinging is common, although in this case, it represented a particular embarrassment for a company that preaches values of openness and transparency. Facebook—itself notorious for its fickle and confusing privacy policies, with each frequent change inevitably exposing more user information—was secretly using a PR firm as a front to drum up criticism of a competing company's privacy practices. Add to that Facebook's creation of what have been called "dark profiles" for people who have never signed up for the service, along with its habit of retaining information that users believed they had deleted, and one gets the sense that the promulgation of a real-names policy is but another element to gather as much information as possible, to make us transparent first and foremost to Facebook and its advertising platform.

## A SINGLE LOG-IN

Not long ago, Web users had more options about how they conducted themselves online. Chat rooms, message boards, and online games



invited us to employ whatever name we wanted. An e-mail provider would give you a mailbox and that was it; it wouldn't scan the contents of your messages in order to provide more relevant advertisements. Even early social networks offered some degree of flexibility, and at the very least, these sites stood alone. Your Friendster or Myspace identity, for whatever it was worth, wasn't connected to a range of other services. These services didn't spread widgets throughout the Internet that allowed them to monitor the habits of millions of people. In contrast, life online was about finding what you wanted and, occasionally, establishing a persona for a particular online community. We trawled the Web relatively unmolested; now the Web watches us and invites, or forces, us to identify ourselves at every opportunity.

Sites such as Quora, a question-and-answer forum where people can come together to solicit expertise or ponder life's big questions, exemplify this shift. As soon as you go to Quora.com, the site asks you to log in with Google, Facebook, or Twitter; if you sign up with your e-mail address, you are expected to abide by the site's real names policy. If you are linked directly to a question, a pop-up message might obscure your view as it prompts you to log in. Click your way past that (it's not easy to find the small link to dismiss the dialogue box) and you might be able to read the first response to a question, but likely no further. The remaining answers will be obscured, unless, of course, you choose to log in with one of your other accounts (or set one up with your e-mail address). The enticement here is that it's easy and that it seamlessly connects to other services you use all the time. For Facebook, Google, Twitter, and LinkedIn, all of which offer these kinds of open graphs or social log-ins, the appeal is obvious: it's one more way for them to spread their power beyond their walled gardens as they follow you wherever you go and collect more information on what you do and who you know.

All of this is a shame. It flies in the face of the more open-ended, freewheeling Web that many of us first alighted upon in the late 1990s. The Web then was perhaps even less civil than what we see now. It

was easy to encounter shady characters in a chat room, or stumble upon a malware site promising free downloads of expensive software. There was also a degree of openness—of a sort totally different from that found in Zuckerberg's remarks, for whom openness is a way for customers to expose their lives to his company—and of intellectual freedom that seems on the verge of being snuffed out, if not subordinated to the sensitivities of Facebook's advertisers. It was a lot like an alternative newspaper (growing up in Los Angeles, I discovered *LA Weekly* around the same time I started poking around the Internet). You could read fascinating dispatches about culture and politics; you could also flip a page and end up smack in the middle of thinly disguised ads for drugs or prostitution. The Web and the alt-weekly were both anonymous, while the latter was free and the former rather cheap, provided you weren't being charged by the minute. Both of these media showed me information that was, at times, a bit beyond my understanding, but I turned out all right. And thankfully, many of my early explorations—through malware, porn, chat rooms, gaming, and elsewhere—didn't contribute to a permanent digital profile, nor were they syndicated in real-time feeds viewable by my friends and colleagues. I was allowed to explore what I wanted to without declaring myself or leaving a trail behind. Looking at something didn't automatically declare my interest in it, or allow a corporation to classify me accordingly and promise to serve me up similar content and ads. I went where my curiosity took me.

"We went from a Web that was interest-driven, and then we transitioned into a Web where the connections were in-person, real-life friendship relationships," said Christopher Poole, the creator of 4chan, the raucous, at times repulsive, but immensely popular online message board, where anonymity is treasured as an absolute right. "Individuals are multifaceted," Poole continued. "Identity is prismatic, and communities like 4chan exist as a holdover from the interest-driven Web."

I would go a step further than Poole. The social web treats everything, every personal encounter or article you read or thing you buy,



as if it were a transaction between friends. Everything is perceived to reflect a deliberate intent—when you're shopping for new shoes, posting on someone's wall, or, whether for research or on a lark, you decide to read *Dabiq*, the Islamic State's English-language magazine. It all is supposed to be part of you, which is why it must be tracked. And yet even this process of tracking has difficulty measuring intent. There is plenty that I do for reasons that I couldn't articulate or that I don't tell my friends or my family, either because I choose not to or I don't think it'd be interesting to them. (And there is much more that I would prefer not to tell companies monitoring my clickstream.) I sometimes act differently in front of my parents than I do in front of my partner or best friend or a police officer. This kind of "prismatic identity" might shock Zuckerberg, who would accuse me of inauthenticity. The truth is that we all do things like this. I have a couple of friends who are comedy writers, and when I'm with them, I become a little more eager in my jokes, looking for anything to riff off of, enjoying the sense that everything is material and that we are all trying to entertain one another. I doubt anyone who knows me would mistake this for insincerity; it's a performance, as one's identity often is, and quite deliberately so in this case.

On an identity-driven, persistently surveilled Web, discrete bits of information matter more for what they say about us and how they inform our public demonstrations of identity. As the Danish academic Anders Colding-Jørgensen argues: "We should no longer see the Internet as a post office where information is sent back and forth, but rather as an open arena for our identity and self-promotion—an arena that is a legitimate part of reality, just like our homes, workplaces and other social arenas in our society." We've moved, he explains, from an information economy to an identity economy. This is a bit self-serving—commentators have developed no shortage of dubious new types of "economy," from the "attention economy" to the "knowledge economy"—but Colding-Jørgensen is onto something. Our consumption of information online has shifted from purely utilitarian to an

expression of the self. This is the paradigm of "Pics or it didn't happen," where every incident is worthless without shareable documentation, because our experiences are made fuller by being shared. Even what we might think of as plainly utilitarian—a recipe, for instance—becomes an object for sharing and identity-crafting. Whereas a decade ago, you might've downloaded or printed a recipe and cooked from it, now you might find a recipe, ask others whether they've used it or have comments, cook the dish, photograph and share the dish on Instagram before eating it, and finally offer a rating or comment on the site where you found it. The relatively straightforward act of finding a recipe and preparing it becomes bound up in complex questions of identity and self-image—Do you want to seem domestic? Do you share this on Facebook or your more exposed Twitter account? Do you take an elegant, well-lighted photo of the prepared meal, or one of your date happily chowing down?

It's these calculations that show how illusory the notion of authenticity is. We can be deliberate in shaping our public presentation, but that doesn't make these gestures insincere. Each of us is engaging in practiced, sometimes Machiavellian calculations about how we want to present ourselves and what we might want to get out of it, and there's no inherent shame in that. Our motivations are complicated, our identities multifaceted. Some of Japan's biggest social networks allow pseudonyms, and yet the country is awash in all sorts of digital interactions and eruptions of new cultural phenomena, from cell phone novels to virtual pets. A person might value his online pseudonym—I still have a soft spot for the one I used for many years in various online role-playing and action games; he exists as a distinct character in my mind—precisely because it is a form of expression, bound to certain experiences. And indeed, handles, avatars, and the other raw ingredients of online identity have long been treated as types of expression and play, things to be tried on and cast off, manipulated and customized. Markus Persson, the creator of the enormously popular game Minecraft, is widely known as Notch, and the nickname is no less real or



authentic because it originated online. His continued use of it, both online and off, only shows how much he values it.

Our digital and offline lives are more intertwined than ever, and in some respects, that's a good thing. These two worlds have never been fully separate. Actions in one arena can easily affect us in another, and the notion that the digital is all illusory has often been employed as a justification for trollish behavior online. A conversation on Facebook is no less real than one on the phone, though each medium offers different possibilities of interaction and may produce varying complications. I might prefer one to the other, but they both exist and whatever I learn in one happened to me as surely as an in-person encounter. What is important is that I have the freedom to do these things and that I am not forced to tote around my Facebook identity just to access other services. Identity shouldn't become an unshakeable shadow.

The ultimate irony of an identity-driven Web where one is pressured to use a single log-in across many sites and apps is that it actually makes us less secure, in more ways than one. Knowing that every interaction is linked to our real-name accounts, we find it easy to become neurotic about what might become part of our digital records or what might be shared, without our consent, on the home platform. Surveillance is nothing if not a form of pressure, in its capacity to cause us to preempt our usual habits, knowing that we're being watched and recorded. It may also cause us to share more in order to alleviate that anxiety, in pursuit of the same nebulous degree of authenticity promoted by Facebook. We feel the need to post more in order to demonstrate our real selves, to overcome the strictures of Facebook's rigid environment.

This instinct also emerges on LinkedIn, where the site features pop-up messages and alerts telling users that they should fill out their profiles in order to make them more complete, to have a better experience, or to "quickly grow your professional network." Information sharing will improve your LinkedIn experience, which will, according to the site's mission, boost your value in the world. Similarly, Facebook

sometimes prompts me to input my phone number; this is for security purposes, the site tells me, so that they have another method of verifying my identity. But in the same dialogue box, I'm offered the option to show my phone number to my friends. That giving Facebook my phone number makes my experience there more secure is, on its surface, somewhat dubious, though the site uses text messages to verify potentially compromised accounts. At the same time, the overlap here of promising security while also encouraging disclosure of one's phone number to friends in the interest of openness or authenticity is revealing of Facebook's motives: the more personal data they can get, the better.*

## NAME AND SHAME

In certain quarters, digital anonymity has become a precious commodity—for dissidents, activists, journalists, and as a cultural value in and of itself. On the social news platform Reddit; in the madcap, all-anonymous message board 4chan; in the hacker collective Anonymous (whose roots trace to 4chan)—in these and other online communities, anonymity is something to be treasured and protected. Chalk it up to scarcity, perhaps. Here an assault on one's anonymity is considered a grave act.

The act of unmasking an anonymous Internet user is often called doxing. Doxing isn't always done on purpose or with the intention of harming someone. Doxing can be accidental or out of the belief that someone deserves to be publicly recognized. It's this very mutability

* And if my account were to be compromised, would I then want my phone number accessible to some hacker? While working on this book, someone logged into my Facebook account from a Ukrainian IP address. I have no idea how it was done, but Facebook locked down my account and notified me via e-mail. I was glad that Facebook acted promptly, but I was also glad that I hadn't given them my phone number or address.



that means that the ethics and eventual consequences may not always be clear. (Whoever doxed J. K. Rowling as the pseudonymous author of the novel *The Cuckoo's Calling* was likely interested in getting more recognition for the book but may not have anticipated how much this act would anger Rowling herself.) Anonymity can be a tool of power or a way to fight against it; it can also be relatively benign. But many of the most notorious cases of doxing are tied to a desire for revenge over some perceived slight. And there are still other instances in which the wrong person has been doxed, leading to harassment. This kind of doxing doesn't differ much from, say, the *New York Post* rushing to name a suspect—recklessly and wrongly, as it turned out—in the Boston Marathon bombing. The goal is the same: make someone infamous, so that they can suffer the consequences. That's why doxing can seem freighted with grandiosity and self-righteousness.

The treasuring of real names, of names as a private thing, brings to mind the use of secret names in traditional oral cultures. Anthropologist Claude Lévi-Strauss famously manipulated members of the Nambikwara, a preliterate tribe in Brazil, into revealing their proper names to him. Among the Nambikwara, proper names were forbidden, so Lévi-Strauss and his colleagues tried to assign what he called "arbitrary appellations," or nicknames, to members of the tribe. (In our own culture, we might think of Internet screen names or the call signs granted to fighter pilots.) In *Tristes Tropiques*, Lévi-Strauss recounts an incident in which he was playing with some children when one girl came up to him and began whispering in his ear: "Out of revenge, the first little girl had come to tell me the name of her enemy, and the latter, on becoming aware of this, had retaliated by confiding to me the other's name. From then on, it was very easy, although rather unscrupulous, to incite the children against each other and get to know all their names. After which . . . I had little difficulty in getting them to tell me the names of the adults."

Essentially, Lévi-Strauss was engaging in what hackers call social engineering, cajoling and tricking his subjects into sharing privileged information. He got them to dox one another and to think that it was

to their advantage. The girl who initially revealed her enemy's name was doing much the same thing. When names are private, when they reveal something fundamental about a person, there's power in revealing them—or threatening to do so.

Like privacy, anonymity is about preserving control over what someone knows about you—in this case, that most fundamental of identifiers: your name. In a networked, data-rich society, knowing someone's name is potentially a way to know all kinds of other things about her. Imagine if you were to walk down the street at all times with a sign above your head telling everyone your name, how to contact you, and other information about your background. That's how we appear to trackers, ad networks, and other companies online.

Doxing is closely tied to the concept of public shaming, which has found new forms on social media. Shaming and viral villainy are made all the easier by the use of real names and the ways in which data travels between social networks. The practice is flexible, as easily applied to an airline that's mistreated a passenger as it is to a relatively unknown Twitter user from Nevada guilty of tweeting a racist epithet. Shaming remains problematic because of its close association with vigilantism and because, in its leveraging of viral channels, it can spin out of control, producing a disproportionate response. The hive mind may respond with a dozen people tut-tutting, only to then melt away, or it may be ten thousand people issuing death threats, publicizing the target's address, calling his employer, and ensuring a permanent data trail of shame and embarrassment—what has been termed "SEO-shaming," after the practice of gaming Internet search results.

When is someone taking the initiative to dox or shame another person a courageous act, or, at the very least, an effort to defend an injured party, and when is it self-righteous or malicious? Such standards aren't clear, in part because, as Danah Boyd notes, "the same tactic that trolls use to target people is the same tactic that people use to out trolls." Both sides in a conflict may be engaging in similar behaviors but toward very different ends.



It's easy for a shamer to come across as a bully, particularly when the shaming is directed at someone with little renown or power of his own. Like satire, shaming seems less effective, and less conscionable, when someone punches down rather than up. In one notable incident, the feminism and pop culture blog *Jezebel* publicly called out a dozen teenagers who tweeted racist remarks after Barack Obama's reelection. The site went beyond posting the tweets by researching the students, writing short bios for each, and contacting their schools. While the students' conduct was abhorrent, they were minors, and the manner in which *Jezebel* went about publicizing their own behavior offered the impression that the act was more about allowing *Jezebel* to grandstand as a moral authority and to rack up page views based on the resulting controversy. *Jezebel* could as easily have contacted the students' schools—the kind of institution of authority that might be able to positively influence the children's behavior, or, perhaps, enact some punishment in concert with the children's families—and written a story about the experience while also keeping the students anonymous. Instead, the site ensured that, for many of these students, they would spend years trying to scrub the Internet of their bad behavior, while likely nursing a (perhaps understandable) grievance toward *Jezebel*, rather than reforming their own racist attitudes. It's easy to forgo self-examination when you, too, feel like a victim.

There's a self-aggrandizing element to public shaming—the unearned self-regard of the mob leader. It tends to privilege dramatic gestures of pique and knee-jerk outrage over quieter or private efforts to engage, educate, and criticize. It can allow one party to call out another's bad behavior, while also overlooking complicating issues of class, power, and influence.

But it's not always like this. At their best, public shamers find common ground with activists whose goal is to show that, contrary to the conventional wisdom that we live in a post-racial or socially progressive society, racism, sexism, and other forms of discrimination are still endemic. It's toward this kind of end that public shamers should dedicate

themselves: surfacing examples of abuse and injustice. Twitter accounts such as @YesYoureRacist and @EverydaySexism or the "Public Shaming" Tumblr are most useful at showing that these phenomena are still very much alive. They allow a wide public to see that discrimination is still often expressed with extraordinary callousness and casualness. They can also provide spaces for people to come forward and share their experiences. Many people are unaware how cruelly women are treated online, especially when they try to speak out on controversial issues. These platforms can be sites of ongoing conversation, where alliances can be made and important issues aren't allowed to recede.

I talked to a couple of people involved in public shaming, partly as a way of working through my own ambivalence toward the practice. I wanted to hear what some of these people had to say for themselves and how they viewed their behavior. Matt Binder runs the "Public Shaming" Twitter and Tumblr accounts. A producer for a political radio talk show, Binder began highlighting racist comments on Twitter in the run-up to the 2012 presidential election. Binder specializes in emphasizing the hypocrisy of some of his targets—for example, he's found young Middle Americans who complain about the laziness of food stamp recipients, only to discover that in the past, these same people have tweeted about being unable to find work. The implication is that these young people are, if not lazy themselves, then victims of the same economic system as food stamp recipients, but their racism and classism leave them blind to this fact. From this kind of myopia comes the site's tagline: "Tweets of Privilege." Sometimes, Binder will pick out racist responses to a news event, retweeting them with an added bit of commentary or arranging a dozen on a Tumblr post and contributing his own sardonic remarks. His efforts have found him a wide audience: when we talked in 2013, @MattBinder had about 11,000 followers, @PublicShaming had 3,000, and his Tumblr, with more than 60,000 followers and surges of traffic around pop-culture mini-events such as Marc Anthony's MLB All-Star Game performance, was sometimes listed among the top 10 most popular pages on



the social network—an impressive distinction for one of the world's most-visited blogging platforms. (Binder also shares his Public Shaming posts on a Facebook page of the same name.) Mainstream news outlets have picked up on his posts, sometimes borrowing them wholesale, and a few ads appear on the Tumblr but only enough, Binder says, to buy lunch once a month.

Binder's presentation mixes righteous outrageous with acid sarcasm. He's happy to mock his targets. "It definitely needs to be entertaining—otherwise people aren't going to pay attention to it," he said. "Social justice blogs and sites like that have been around a long time. Not every one of them has blown up as big as this site has."

At the same time, he recognizes that some online opprobrium is unlikely to provoke contrition: "A couple people telling them online that they're idiots isn't going to change their outlook." Instead, he sees his role as surfacing incidences of hate speech and making them visible to a wider audience, even if the person making those remarks doesn't understand their impact. "A lot of people don't even realize what they're saying," he said, "and even when they do, they don't seem to have a problem with it, so they double down on it. It's kind of shocking." Binder's site then exists more as an example to others, particularly liberals who may have developed some sense of complacency about social progress. Many of his readers, he said, also aren't politically attuned and may not be aware of the kinds of opinions spouted on social media. "The point of the blog is sort of to show people that these opinions exist and these types of people still exist."

I asked Binder how he responded to accusations that his site was self-righteous or damaging to those he targets. He was unconcerned, explaining, "I don't really care about bullying people who are assholes." He added: "If you saw a kid getting bullied and you went and stood up to [the bully], would you be considered a bully because you stopped" it?

Binder doesn't believe in censoring the vile remarks of others, but he does have some limits. He won't go after anyone who "looks especially young." He doesn't pick out anonymous or pseudonymous

accounts, because he wants to show people who are willing to broadcast their awful opinions under their own names (and, often, with a photo of themselves attached, along with other personal information).

Logan Smith, who runs the @YesYoureRacist Twitter account, has shown more leniency. He retweeted someone's racist comments only to backtrack after seeing that the man's account contained some remarks about suicide. "I really don't want to be responsible for pushing someone over the edge," Smith told me. Another man was in basic training in the military; he apologized to Smith, and though Smith doubted his contrition, he removed the tweets because he didn't want to jeopardize the man's career.

Smith went to college in South Carolina and lived there afterward for another four years. Every day when he drove to work, he said, he drove by the state capitol, where the Confederate flag still flew. A local barbecue restaurant chain also flew the flag and distributed segregationist literature. Later, he moved to Raleigh, North Carolina, where he's found work in progressive politics. The racial climate is somewhat better there, but he still lamented the state's passage of a restrictive voter suppression law. There's something in common between Smith's everyday activities—his political activism and the institutional racism he's observed in these communities—and his Twitter project. (When we spoke, Smith said he was working on a book project that would also examine the history of racism in public policy in the South.)

His account is particularly interesting because he seeks out people who start by hedging their comments—"I'm not racist, but . . ."—only to spill out remarkably prejudiced comments. Each of these tweets arrives with a sort of cognitive dissonance baked into it—a prophylactic denial of being racist followed by a clear example of that very sin. Smith explained how widespread he's found this phenomenon to be: "It's really opened my eyes to how many people, especially young people, don't seem to understand the concept of racism. It seems like they think that unless you're out there lynching somebody or burning a cross in someone's yard, then you're not a racist." Smith's not as gleefully belligerent as Binder (the two aren't well-acquainted but spoke respectfully of each other; they've also had contact with other people using social media to highlight homophobia and racism); but he has a similar attitude toward the cause. "I'm not at the forefront of the civil rights movement," Smith said. "I do not have any illusions about that. I simply found a simple method of publicizing racism."



Talking with Binder and Smith left me feeling more approving of their efforts, though the former's enthusiasm, as well as his self-identified status as a bully for a good cause, left me a bit uneasy. Perhaps it's that they operate from a position of security—liberal white men upholding respectable values by pointing to the buffoonery of others. They're not risking much, and they are mostly preaching to the converted. It's possible to detect a halo of sanctimony, though Smith's experience in progressive politics showed him to be a thoughtful activist. But there's no doubt that the comments that they seize on are vile, and there's something to the claims that many people, especially young people, seem to think that their online racism is somehow hidden or doesn't count as racism, particularly if it's presented with a caveat. Exposing racism is, on its own, a laudable goal, and there should be some social cost to being a bigot, no matter the form in which it's presented.

Shaming can be effective if it's directed toward worthy targets—corporations guilty of discriminatory behavior, powerful figures who deserve to be called to account, a pattern of destructive behavior by a community leader that has received insufficient attention. A random Twitter user with a few hundred followers, unused to being in the spotlight or interacting with traditional media, will likely recoil in the face of a public shaming. He'll adopt a defensive posture, as his friends rally around him or laugh at his sudden exposure. He might delete his Twitter account, as did many of the students shamed by *Jezebel*. And he might be more guarded in his public postings, which by some measures would constitute an improvement. But he's unlikely to embark on any real soul-searching. Shaming people in positions of influence strikes me as more useful in fomenting social change.

The court of public opinion, however, is likely to be an increasingly busy place in the coming years. Going viral can be seen as a threat, as Taylor Chapman thought when she filmed her tirade at Dunkin' Donuts. In an online environment in which we are always visible and named, reputation is an increasingly valuable commodity. Damage to one's good name can seem equally perilous, which is why so many online disputes escalate so quickly and why their private, muted resolutions receive less attention than their explosive beginnings. Given a traditional legal system that often seems rigged for the wealthy and the powerful, online speech, despite its quirks and limitations, feels like a more honest, democratic place in which to litigate one's problems. Our ability to exact justice or defend ourselves, it can seem, is only limited by our eloquence and appeals to reason and emotional honesty. Unfortunately, that's not always true; the fallacy of social media as an inherently meritocratic, democratic space cuts both ways. Corporations are making their own efforts to game social media to their advantage, employing sentiment analysis, consultants, and always-on PR and social-media representatives to nip any crisis in the bud. Your complaints about mistreatment by an airline may mushroom into a mainstream news story, or they may be snuffed out by an attentive social-media marketing officer, who responds to your tweets, monitors your mentions, and strategically buys sponsored tweets to appear in your followers' feeds. A campaign against an offensive newspaper columnist may fall apart as his powerful colleagues fall into step behind him, leaving the protesters less powerful than when they began. And once made, accusations can't be withdrawn. They can only be revisited or corrected, followed up upon in the same way we often over-share to make up for some crappy joke or faux pas we suddenly regret. Meanwhile, some archival record lives on: in search results, in someone's screenshots, in the disembodied audience to whom we've made our appeals.

What's the end game? What kind of consequences do we want for the shamed? More speech is usually a good thing; bad speech can be countered with good speech, our liberal impulses tell us. But that is again to assume a level playing field. As it is, the cyclonic effect of social media, its tendency to act as a perpetual outrage machine, can be wearying. Depending on the size of your networks, you may be used to seeing another scandal, another villain, every day. These overheated campaigns tend to run together, even as each provokes a need to comment, showing that we care and that we are on the right side of—well, not history, but some progressive sensibility shared by others in our timelines. There's certainly a place for shaming and declaring your anger, as there is for other forms of protest. Sometimes we need to point at something and say, this is it, this is the thing itself, we must do something about it. But in a mediascape where attention is scarce and valuable, there is power in refusing to grant it.



## THE MERITS OF ANONYMITY

The safety of a pseudonymous Twitter account might encourage some people to be trollish, but it also allows for the ability to speak freely without fear of consequence. A future political commentator might find his footing by starting out under a pseudonym. A woman used to being harassed online might find a respite by shedding her female identity for a while or adopting a new name. It allows us to determine who we are on our own terms. To that end, given the increasing recognition of gender as fluid and gender identity as something personally defined and mutable, it is surprising that it took Facebook a decade to add gender options besides male and female. Its introduction of a few dozen different gender options is an improvement but far from the ideal, and simplest, solution: a blank box, in which users can decide what they want to write, if anything at all.

Anonymity need not be seen as only a form of digital refuge. In a society besotted with publicity and granting credit for everything, it can be liberating to reject all of this. Anonymous expression has a

rich tradition, from the Federalist Papers to graffiti. An anonymous publication can also have the feel of being a stunt, as evidenced by the speculative furor surrounding the identity of the author of *Primary Colors*, before it was revealed to be the work of *Time* magazine journalist Joe Klein—someone surely familiar with the machinations of publicity and media fame. That said, writers such as Stephen King and Doris Lessing have published novels under pseudonyms in order to see how the works might be judged. And in a surveillance society, where power is known to act capriciously, the right to anonymity, and anonymous expression, should be treasured. Anonymous protest is both a prudent tactic and a savvy way of keeping attention on an issue, rather than the people engaged in some act of subversion. In the process, the markers of anonymity—such as the Guy Fawkes masks worn by the Anonymous collective and other loosely associated leftist protest groups—help to bind individuals together as part of a community devoted to a larger purpose.

Anonymity can also improve digital security, especially when your digital persona is networked across so many platforms. A hacker might gain access to one of your social-media accounts only to find that they can use it to log into numerous services, essentially gaining control over your entire digital life. Do you know how many apps you've authorized on Facebook or Twitter? Do you know what each of them is allowed to access, and what each app's data-sharing policies are? Probably not, but don't be hard on yourself: these permissions settings have become like the terms of service agreements that we all consent to every day and that almost none of us reads. And even these agreements are often broad and intentionally vague, so that an app or site claiming that it will only share your data in ways meant to provide you with more relevant services can easily translate to: We'll sell your data to whoever comes calling. One study examined fifty health and fitness apps and found that the free apps were more likely to sell personal data—information that would be less valuable, and less harmful, if it's not tied to your real name and social-media profile. Consequently,



it's important to keep a close eye on these apps, particularly on ones you haven't looked at in a long time, because you don't know what they might do with your data. Like the popular Facebook groups that suddenly and surreptitiously change from supporting some charitable cause to promoting a credit card, third-party apps and sites may find themselves under new, less scrupulous ownership. By accepting the terms of service agreement for Facebook's own Messenger smartphone app, you authorize the app to make calls, send texts, take photos, record audio, read your contacts, read your call log, and look at personal information in your device settings. (The app also requires users to opt out if they don't want the app to automatically append their location to each message they send.)

The battle between real names and anonymity need not be zero sum. Unfortunately, Facebook and Google have done their mightiest to make it so. But remaining anonymous and presenting oneself publicly should be practices that can coexist. As in the physical world, one should be able to move between digital spaces that are anonymized and others in which one's real identity is needed and useful. But the trend is clear: anonymity is under assault. If the positions were reversed—if, perhaps, Facebook had a financial interest in preserving anonymity as a value and technological capacity—then it might be the single-identity faction who would be demonized and would have to defend their practices. Theirs, after all, is the more stringent ideology. But that is not how the powers are arrayed. Anonymity certainly has a public relations problem, and some defenders of anonymity haven't done enough to recognize how anonymity can be a facilitator of some of the worst behaviors of online abusers: death threats, misogyny, stalking and verbal abuse, racism, and so on. But it's also important to distinguish between that which anonymity enables and that which would be otherwise impossible without the ability to be anonymous. Most of these horrible behaviors are not solely a product of anonymity, much less a shared value of those who do believe in defending anonymity. Some people choose to act in such a way because they know they can

hide behind the protection of a pseudonymous Twitter handle or a 4chan message board in which no one is ever identified. But these actions often take place online anyway, just as they do in the analog world. Anonymity may occasionally be a shield for sexual harassment, but it's not a cause. To stamp out anonymity with the intention of making a more civil or humane online environment is to choose a technological solution that merely papers over the underlying social and political problems. Rape culture, misogyny, the marginalization of minorities—all these and more can't be fixed by making people register for Facebook under their real names. Plenty of real-name social-media accounts are the bearers of despicable messages, as are talk-radio hosts and mainstream politicians. Features to report abuse and block users are therefore necessary and helpful in policing bad actors. But the major social networks have become victims of their own rhetoric. In promoting Facebook as an electronic agora of limitless connection, Facebook has created a sanitized version of human life, one that bears little version to the physical world it claims to represent. It has also helped to create a digital culture which, rather than working to tackle existing social issues, often devolves into a cacophony of anger and recrimination whenever an unsavory person finds himself with a megaphone—a cycle that can lead to calls for further clamping down on digital speech. Facebook and its users would benefit from recognizing that, if the company hopes to link people together in massive numbers, a range of behaviors will inevitably appear, because that is how human beings act. Trying too hard to guide these behaviors is likely to result in manipulation and a crackdown on anything but the most prudish forms of speech.

## THE POWER OF REAL NAMES

It's important to understand the motivations of those calling for real names online and the potential future implications of these practices.



When Arianna Huffington said that anonymous comments must be abolished on the *Huffington Post*, the enormously popular news site and aggregator she founded, she was calling for a change in policy that would serve her own business practices. If HuffPo were to adopt real names, say, by replacing its commenting system with one provided by Facebook, it'd immediately become both a partner to the social network and a node in its data-collection apparatus. HuffPo would then be able to build up even more data about its millions of monthly readers. It would know even more than it already does about who they are, what they read, what they buy, and what they think. This information would be helpful for the site's targeted advertising efforts, and it'd be quite valuable to commercial partners. It also would offer another tool for banning unruly commenters.

Banning anonymity is, in short, a strategy of the powerful. At minimum, it allows for greater data collection or control over a communications network. At its worst, it's a tool for authoritarian governments to monitor and track their citizens. That's not to say that governments don't like anonymity—when it serves them. For decades, U.S. presidential administrations have employed anonymous leaks in order to plant stories, guide public opinion, or stave off controversy. Despite occasional harrumphing from critical journalists and media observers, the practice of anonymous sourcing continues because national security journalists fear losing access or being scooped on a story. Tor, the free anonymizing software that allows for covert Internet browsing, was originally sponsored by the U.S. Naval Research Laboratory to help democracy activists communicate overseas. Another U.S. government agency, the NSA, has been trying to break the Tor network ever since.

There are, of course, many other instances in which we'd like to preserve anonymity: voting, visits to doctors or lawyers, double-blind medical studies, buying porn or a gift for a friend. Anonymity can also be a way of removing certain motivations—greed, ego, vanity—from practices that might be better served by a form of silent cooperation or unacknowledged altruism. Maimonides, the twelfth-century Jewish

polymath, ranked various levels of tzedakah, or charity. Among the highest levels was a donation where neither the giver nor the recipient knew the identity of the other party; they're anonymous to each other and so no one can claim excessive pride or credit. The recipient also retains some dignity by not having to know the donor. The expression of charity can stand alone, just as an anonymously published essay or a pseudonymous Twitter account can be judged on its own merits, without worrying about the confounding roles of follower counts or influence metrics. Anonymous online speech mitigates some of the obligations that come with digital publishing: incessant promotion, worries about audience composition, appeals to the whims of advertisers and members of one's peer group or professional network.

In a time of precarity—widespread unemployment, record income inequality, rapid technological change, looming environmental calamities—identity has become ever more fixed. One would think that it should be the opposite—that with society, and job markets in particular, in such a state of flux, people should have more flexibility to define themselves as they wish. Perhaps you are a Muslim immigrant living in a midsize American city and wouldn't mind posting background information on your Facebook profile. But then your neighborhood begins to feel the effects of a recession: houses foreclose; crime goes up; a neighborhood watch group forms and soon starts spouting noxious anti-immigrant rhetoric. You might decide, with some reluctance and sense of inner conflict, to change your name and avatar on Facebook to something that won't mark you as Muslim. Again, you may not feel good about it; but perhaps that's what you choose to do so long as your neighborhood feels unsafe, or before you can move, or before you can try to rally some neighbors to support you or talk with law enforcement. Under Facebook policy, you would be allowed to do no such thing. What's more is that if you attempted to make a similar change with other social-media accounts and the various online services to which they're connected (at the time, having your Facebook log-in as a near-universal Internet ID seemed so convenient),



you might run into a host of competing policies, with most of them tending to push you give them as much information as possible.

Consider another scenario in which you were fired from a job doing data entry for twelve dollars an hour. Your boss was actually a real pain—among other things, he was always pressuring you to have drinks with him after work—and it led to so much friction that eventually you were let go. Perhaps you want to be able to post an anonymous review of him on a job board, without fear of retaliation, or simply to vent anonymously (and without naming your ex-boss) on your Google+ account. It was also the kind of experience that you don't want to explain in future interviews; it was only a couple of months of low-wage work, and you believe that it's your right to withhold this information from another employer. Yet by the logic of LinkedIn, you would disclose all of your employment information, along with your educational history, your entire career network, and every skill in your quiver. Your account also would be viewable by anyone who happens to search for you on LinkedIn. Sure, it's a truism that people fudge their résumés, but wouldn't a little obfuscation, some strategic elision, be understandable here? And wouldn't you also want to look for a new career without your imperious ex-boss looking over your shoulder? On LinkedIn, you can't: the site tells you who's been looking at your page. It doesn't even include a block feature—a design choice which, along with the site's tendency toward high-volume spamming and too-intrusive "you might know" reminders, has earned it the label of "the creepiest social network."

It's in conditions very similar to these that Internet entrepreneurs in recent years have been touting the virtues of public identities that serve as advertisements for yourself. Developing a personal brand, selling yourself, maintaining public profiles, monetizing the things you already have, be they underutilized expertise or a spare room in your house—the good neoliberal subject is someone who is always hustling and available. Among the most popular products in this "sharing economy," as its partisans call it, is Airbnb, a service that allows people to

rent rooms, houses, and apartments directly to each other. The idea is that the supposed inefficiencies and extra costs—taxes, insurance, maintenance—of hotels can be bypassed. Your house is going to be empty for a week anyway while you're visiting your in-laws; why not rent it out? There are problems with this kind of economic philosophy, which I'll get to later. But first, consider the unintended consequences of these kinds of transactions, which rather than being anonymous, cull information from social-media profiles in order to bring people together.

One of the nice things about booking a hotel over the phone or online is that they don't know much about who you are. Yes, hotels may be collecting some data behind the scenes, perhaps to market to you better in the future, but they have no interest in turning you down as a patron, nor do they have the legal right to do so based on your identity.

Those rules don't quite apply with Airbnb, which encourages users to log in with their Facebook accounts and provide detailed profiles. Some Airbnb users have reported being discriminated against because of their appearances. Franklin Leonard, who owns the Black List, a script discovery and reading service in Hollywood, recounted to me a story about trying to book Airbnb lodging for a business trip. Leonard travels frequently and had had success with Airbnb in the past. Six months before a film festival, he tried to rent a house in Austin for himself and several employees, but the owner refused, saying he wouldn't rent anything more than three months out. Leonard offered 20 percent above the list price but was rebuffed. Three months later, he tried to rent the same house and was rejected several more times, despite offering to pay well above the listed rate. Leonard was baffled. He e-mailed the owner asking what the problem was. "He responded by saying that he wasn't not renting it to me because I was black and that he had rented it to a member of Jurassic 5 only recently," Leonard told me.

It was the e-commerce version of "some of my best friends are black." The homeowner was conscious that his behavior *appeared* racist, so he tried to preempt it by saying that of course his decision wasn't racially motivated. But the message had already been communicated: Leonard and his employees weren't welcome there, and the reasoning was fairly clear.



Leonard began changing how he styled his Airbnb profile. "As it is, I do everything I can to make clear that I'm a responsible tenant," he said, "typically either mentioning that I'm in town with the company that I founded and run or that I'm traveling with my fiancée.

"After this event, I actually changed my profile photo on Airbnb to one with my fiancée [who isn't black] and I together. Sad but true. Got the idea from another black man on Twitter who had had similar experiences."

Despite tweeting a complaint at Airbnb, which encourages Twitter feedback from users, Leonard never heard from the company. He had little recourse but to take precautions in how he presented himself—to, oddly, show less of himself on a site that encouraged him to be himself. And his experience isn't unique: one study by researchers at Harvard Business School found that black hosts charge on average 12 percent less than nonblack hosts for comparable rentals. The study concluded that black hosts have to charge lower prices in order to overcome the racism of some renters. The authors also recommend that Airbnb adopt measures similar to those of online marketplaces such as eBay, where sellers and buyers don't need to share their photos and names.

Racism disappears no more with anonymity than it might with face-to-face encounters. But stories such as Leonard's provide a reminder that the promised bonhomie of transparency can be elusive. Rather than bringing people closer together, insisting on furnishing full identities in situations such as these can lead to discrimination, abuse, or other fractious social behavior. A person's authentic self may be a racist one. Sometimes people don't want or need to be seen, and there are good reasons for that, which should be respected. Anonymity can be a refuge. It can also just make life easier, which is why booking

a hotel online is more frictionless than negotiating the personalized stalls of Airbnb.

The German film director Werner Herzog once said in an interview, "We have to have our dark corners and the unexplained. We will become uninhabitable in a way an apartment will become uninhabitable if you illuminate every single dark corner and under the table and wherever—you cannot live in a house like this anymore." Herzog, a delightful eccentric, was railing against psychotherapy. But while his antipathy toward Freud's science might be overblown, his point is equally applicable to digital life. The social web combines a confessional society—with its privileging of openness and self-revelation for its own sake; its equating of brute honesty with virtue—with the totalizing demands of a surveillance state. When we are always identified, we step further down the path of the totally illuminated world that Herzog fears. We don't need to revere subterfuge, being withholding, or even lying, but we don't need to eliminate these things either, whether by custom or a programmer's directive. We need to allow for ambiguity, the freedom to do wrong, the freedom to be not yourself but some other self. Shade gives texture to life's landscape.

In the same interview, Herzog also expressed some appreciation that there are many false versions of him on the Internet—people imitating his distinctively dour German accent on YouTube, fake Herzogs planting flags on deceptively official-looking Facebook pages. "What it's about I don't know," he said, "but I welcome it, because I see them as some kind of protectors around me. As though they were bodyguards." Herzog is speaking from a position of privilege—he's a successful director of art films who's never cared about the expectations of others. But there's something wonderful about his philosophical bent. He's unintentionally offering a defense for the practice known as deliberate obscurity, putting out false traces and concocted data trails to give would-be surveillers a misleading sense of who you are. His words also call us to tolerate uncertainty, to find that there can be something weird and interesting about not knowing who we're dealing with or



who even might claim to be us. This sentiment is the animating joy behind the verve for strange bots—performance art projects, moody spam bots, automated accounts that mimic our tweets upon request. Of course, there can be consequences of such practices—identity theft comes to mind—but we might also discover a measure of freedom by surrendering some concern. We would replace the cynical, verify-yourself skepticism of the current moment with something more creative, unbounded. Along the way, we might even regain a measure of security, for acknowledging identity as fluid and self-directed would make for a more interesting, and trusting, culture.

To reach such a state would require that our actions online go untracked, much less be used against us in ways we don't expect. Unfortunately, an entire industry has built up around doing just that.