

# 1

## The Privacy Virus



JAMES GRIMMELMANN

**H**ow many times have you heard someone (probably someone over forty) say, “Kids these days don’t care about privacy”? Facebook is their Exhibit A: over four hundred million users and growing, telling the world all sorts of scandalously personal details. And it’s not just keg stands, either. There are things federal law considers so private it’s illegal to ask you about them in a job interview. Age. Sex. Birthplace. Religion. They’re all questions on the *first page* of the Facebook profile form. Yea, verily, privacy is dead and the kids these days killed it.

It’s a neat theory, except for one inconvenient detail: the actual behavior of Facebook users. If “privacy” is on the list of words nobody uses any more, Facebook users didn’t get the memo. College students spend the wee hours of weekend nights untagging photos of themselves on Facebook, removing the evidence of their drunken revels earlier in the evening. A “Facebook stalker” is a creep, not a contradiction in terms.

In fact, as you look closer and closer, the idea that Facebook is privacy’s tombstone becomes stranger and stranger. If over four hundred million users don’t care about privacy, why are they using a site that allows them to reject friend requests? If they wanted to broadcast every last detail about their lives to everyone everywhere, why don’t you ever see credit card numbers on Facebook profiles? And why did hundreds of thousands of users sign petitions protesting Facebook’s decision to introduce real-time news feeds? For people who allegedly don’t care about privacy, Facebook users sure spend a lot of time worrying about it.

Challenge a Facebook skeptic on the lack of evidence for her claim and she'll usually retreat to one of a few related backups:

**1. Actions speak louder than words.** Anyone can *say* they care about privacy, but when it comes time to actually *doing* something about it, there they are on Facebook, posting incriminating photos and salacious stories.

**2. Actions have consequences.** Wanting privacy on Facebook is like training for a marathon by drinking gasoline; you'd only try it if you hadn't thought things through.

**3. Youthful indiscretions.** Facebook users care about privacy only after they've learned their lesson the hard way.

These replies may sound more plausible, but they all have something in common: contempt for Facebook users. If you say you care about privacy but don't, then you're a hypocrite. If you don't reconcile your desire for privacy with the facts of Facebook, then you're stupid. If you haven't yet had a bad experience on Facebook, then you're young, lucky, and foolish. These attitudes—which, to be fair, are rarely stated so baldly and insultingly—all presume that Facebook users simply haven't seen the truth about privacy that the dismissive skeptic has. She's right, you're wrong, end of story.

Actually, it's the skeptic who has things wrong about privacy on Facebook. Facebook users do care about privacy, and they do try to protect it on Facebook. The skeptic goes wrong when she assumes that "privacy" can only mean something like "keeping things secret." It doesn't—privacy is much richer and subtler than that. Privacy is a key component of being free to be yourself, building healthy relationships, and fitting into a community that values you. Facebook users care about *contextual privacy*:<sup>1</sup> they want others to respect the rules of the social settings they participate in.

### Private and Public

Let's start by asking what the skeptic is thinking of when she talks about "privacy." If we pressed her for an explanation, she might

---

<sup>1</sup>The idea comes from privacy theorist Helen Nissenbaum, who calls it "contextual integrity."

say something like “the right to be let alone,” or “I don’t want my personal life on Entertainment Tonight,” or “you can’t come in without a search warrant.” These ideas all depend on an implicit *theory* of what privacy is: “private” is the opposite of “public.”

The underlying idea is that the world can be divided into two spheres: one that’s out in the open and shared with others, and one that’s behind closed doors and shared with almost no one. The daytime world is the public sphere. That’s where politics, news, work, and the mass media are. The nighttime world is the private sphere. That’s where home, family, and friends are. The public is extroverted and loud; the private is introverted and quiet. Public is visible; private is hidden. Everything is one or the other.

As a theory, it has a natural logic to it. Things you do in “public”—that is, in public places or where all sorts of strangers can see you—are fair game for anyone. Things you do in “private”—that is, in your home where no one can see—are off limits. When a celebrity pleads with the paparazzi to stop following her, she’s typically upset that her “private” time with friends and family is being turned into “public” news and entertainment. The police can trail you freely when you’re out walking in “public,” but they need a search warrant to enter the “private” space of your home.

Drawing this bright line between “private” and “public” means that privacy is a close relative of secrecy. Private information is secret information: just you and a few close friends and family. If someone tries to make it public without your consent—the paparazzi, a blackmailer, a creepy neighbor who steals your diaries—the legal system will step in and protect your desire for privacy. But once you voluntarily choose to give up secrecy, by going out in public or publishing your writings, the cat is out of the bag and the legal system won’t help you put it back in. The choice is yours: you can keep your secrecy or give it up. But you have to choose one or the other, no waffling.

Given that the skeptic sees privacy in these terms, let’s look at Facebook through her eyes. She might start by trying to decide whether Facebook is a “private” or a “public” space. (Obviously, it’s not a physical space like a living room or a restaurant, but it is enough like a place that we feel comfortable saying things like “Scrabulous used to be *on* Facebook before Hasbro made them *remove* it; then it *came back* under a new name.”) With more than four hundred million users, the obvious answer is “public.” Your computer is a private space; Facebook is a public one.

Or, she might ask the question in terms of secrecy. How secret have you kept your photo albums and your favorite movies? Obviously, not completely secret, or you wouldn't be on Facebook at all. In fact, the whole point of being on Facebook is to share things, isn't it? And you have, what, three hundred Facebook friends? That's an awful lot of people. Benjamin Franklin said, "Three may keep a secret, if two are dead." Barring mass murder, three hundred people can't keep a secret, period.

That's why the skeptic's first conclusion is that Facebook users must not care about privacy. They're posting lots of personal things about themselves, and according to her theory of privacy, posting something to Facebook makes it public. Therefore, Facebook users are deliberately giving up their privacy in all sorts of personal information. Q.E.D.

Her theory of privacy as secrecy also explains her reaction to the news that Facebook users *say* they care about privacy. Regardless of what they say, they're not treating all their personal information as though it were a closely guarded secret. Thus, her theory explains, they don't consider any of it private. That leaves a gigantic contradiction between their words and their deeds.

### Why facebook?

Her logic is flawless, but she's starting from a flawed assumption. Privacy isn't just about secrecy. When Facebook users fill out detailed profiles, post embarrassing videos of each other, and admit to horrible indiscretions in their status updates, they're still thinking about privacy. Indeed, they're taking steps to protect their privacy, *as they understand and care about it*. To reconstruct what privacy means to many Facebook users, let's look at how and why we use Facebook.

The first thing you do when you join Facebook is fill out your profile. Upload a picture to show what you look like. List some of your favorite books and movies. Say where you live, where you went to school, where you're from. Take down that boring photo and replace it with one of you doing a headstand when you were eight, or making peace signs with your best friends. Start cracking jokes in your profile; rather than just saying you're a fan of the Daily Show, use a Jon Stewart quote in your interests section. Be creative. These are all ways of establishing your *identity*, of saying who you are.

*The Privacy Virus*

7

Next, you need to start friending people. Facebook can crawl your address book to find people you know already; it can also make suggestions based on who it thinks you might know. As you meet people in real life, you can add them on Facebook. Once you're connected, you can send each other wall posts, pokes, gifts, and invitations to play the latest game fad. These are all ways of building *relationships* to other people.

As you become an experienced Facebook user, you may graduate to some of its more advanced tools and applications. You can create events and invite whole groups of friends to them. You can sign up for causes with other like-minded folks. Perhaps you'll join a team of thousands in a game; or upload an album of photos from a party so that all your Facebook friends can tag and see each other. These are all ways of being part of larger *communities*.

From start to finish, these three kinds of motivations—identity, relationships, and communities—are all profoundly social. There's a reason Facebook is called a "social" network site. When you're saying who you are, you're performing for an audience of your friends. You can't have a relationship without someone else to have the relationship with. A community of one is a boring community. The really good reasons to use Facebook all involve other people.

This shouldn't be a surprise. Why did you join Facebook? Because of its cool blue-and-white color scheme and wide range of applications? Probably not. If you're like most people, you joined Facebook because that's where more and more of your friends were, and you wanted to join them. Facebook is about connecting with people.

**Contextual Privacy**

So here's the thing: Connecting with people always means giving up some control over your personal details. "Social" and "secret" don't work together. Whoever you interact with is going to learn something about you. Buy a pack of gum at the newsstand, and the guy behind the counter will learn what you look like—and that you like gum. Watch a movie with friends and they'll learn something about your taste in movies. Make jokes on their Wall and they'll learn something about your sense of humor. You can't get a life without giving something in return.

What this means is that "privacy" is also inherently social. That's true about identity too: you're a different person at work than you

are at home, and a different person again when you go out on the town with your friends. And it's true about relationships: If everyone knew everything about everyone else, couples couldn't say "there are no secrets between us" as a way of establishing intimacy. And it's true about communities too: the Masons have a handshake that outsiders aren't supposed to know, while everyone from New Haven knows where the best place to get *real* pizza is.

In all of these social settings, privacy is meaningful because everyone involved knows the rules. Not because they were given a brochure with the "rules" of friendship, but because in our ordinarily social life we understand what's appropriate and what isn't. If you run into the guy in the next cubicle at a club, don't mention it the next day in front of your boss. Don't kiss and tell. Don't bring out-of-towners to the bar. And so on.

These implicit rules help define a set of social contexts. At home you're in one context, at work another. A walk in the park with a friend is one; a trip to the supermarket is a different one. One way of thinking about privacy is that your behavior in one social context only makes sense *in that context*. When someone takes information from a social context and decontextualizes it—publishes the details of your pillow talk, say—they're violating your privacy.

For you, it feels like being exposed to the hurtful disapproval of outsiders who don't understand what it was really like. For society, it threatens to break down the trust and social glue that make our millions of different social contexts possible. That would be a huge loss. It would mean you could never really be yourself in your free time, that friends could never really trust each other, and that all sorts of vibrant communities would break down. Privacy and social life itself depend on respect for the barriers between social contexts. What happens in Vegas, in other words, needs to stay there.

This isn't an ironclad rule, of course. Teenagers violate each others' trust all the time, and the world hasn't ended because of it. Contextual integrity, though, does explain why they get upset when it happens. It also explains a lot of privacy-protecting legal rules. The police can't come into your home without a search warrant; that's because your home is, like many other places, a natural social context. Your doctor can't go on the evening news to talk about your rash; that's because the patient-doctor relationship is a social context in which personal attention and trust are essential. You can't hack into people's email accounts; that's because reading

their mail would let you butt in and spy on all sorts of social contexts you weren't invited to.

A fuller understanding of social contexts improves on the skeptic's theory of privacy-as-secrecy because it recognizes that privacy isn't black and white. Instead of two social contexts—everything has to be “private” or “public”—it recognizes that there are many. Some are small (a conversation between twin siblings) and some are large (a comics convention with a hundred thousand attendees). What matters is not how many people know something, but whether the implicit rules of privacy in a social context are respected.

### **Contextual Privacy on facebook**

Turning back to Facebook, we have a better answer to the skeptic. A Facebook user who declines friend requests from colleagues at work is taking her privacy seriously; she's trying to preserve the boundary around the social context of her profile and her wall. Students who untag photos of themselves doing keg stands are trying to keep intact the social context of the party by preventing it from blending into the social contexts of their classrooms and families. When someone tried to blackmail Miss New Jersey using photos from a friends-only album, she was rightly horrified that, in our terms, someone would abuse the social context of her friends network.

And take News Feed. The Facebook users who protested the initial launch of News Feed were furious that Facebook took what they thought were relatively “private” acts (a change in relationship status, a comment on a friend's wall) and made them visible. Facebook apologized and added options to keep various items out of your News Feed, but then a strange thing happened: most users didn't use the options, and the anger died away.

The skeptic would cite this story as proof that Facebook's users don't really care about their privacy and just like to complain. From a contextual-integrity point of view, though, their anger and acceptance both make sense. They were outraged because when Facebook launched News Feed, it was changing the rules in the middle of the game, like a teacher who confiscates a passed note and forces the students to read it aloud. That violated users' understanding of how the social contexts of Facebook were supposed to work. After News Feeds had been around for a few weeks, though,

users had time to learn how they worked and adjust their expectations accordingly. You might be a little less free in what you say on someone's wall, now that you know it'll end up in your own News Feed. But that, you can live with. Once users understood the new social contexts—and once they decided Facebook wasn't about to yank the rug out from under them again—everyone chilled out.

Facebook users, in short, do care about privacy. They're having real, meaningful social connections on the site. They bring to those connections most of the same expectations of privacy—that is, expectations of contextual integrity—that they bring to the rest of their lives, offline and on. Using Facebook is not a sign that they've chosen to throw privacy to the winds.

### The Privacy Virus

There's a twist, though. Even though the skeptic may be wrong about Facebook users, she's not wrong about Facebook. Even if its users don't mean to compromise their privacy when they use it, it still happens with alarming regularity. A ticket-taker for the Philadelphia Eagles loses his job after posting a Facebook status update complaining about a recent trade. U2 singer Bono cavorts with two young women whose combined ages don't even add up to his; the tabloids find out everything from a "private" Facebook photo album. A man buys his wife a ring for Christmas, only to have Facebook push the news out to his News Feed, which she sees. Lots of people who really do care about privacy have been burnt by Facebook. It's a privacy disaster zone.

What went wrong? In a sense, the problem arises precisely because people use Facebook socially. They bring to it the same kinds of hopes and expectations they bring to other social settings. They want to have the same rich, complicated friendships online that they do face-to-face. Since they also care about privacy, they rely on the same rules of thumb they use to evaluate privacy risks in daily life—all the adult equivalents of "Don't talk to strangers." The problem is that these rules of thumb, finely-calibrated by many years of experience to help us navigate familiar social settings, can break down badly in the alien landscape of Facebook.

Thus, for example, one of the cardinal rules of social life, one so deeply engrained that we use it all the time without the slightest thought, is *know your audience*. You wouldn't tell the same jokes to your parents, to your boss, to your kid sister, to the man



next to you on the bus, to a cop, or to someone you've met in a bar. Instead, you take a quick, subconscious glance around to see who's listening, and you tailor what you say to fit. Fart jokes make terrible pickup lines.

Facebook users go through the same mental calculation every time they log in. How should I word my status update? Is this video safe to upload? The problem, though, is that it's hard to know an invisible audience. Take a moment to try to imagine your entire network of friends. Who'll be able to see your next status update? How many of them can you name? Even if you know that your grandmother is a Facebook friend, do you remember that fact every time you post? Every time someone forgets (and it's easy enough, given that their grandmothers probably aren't regularly commenting on their status, the way that many of their other friends are), that's a potentially embarrassing privacy slip-up right there.

Here's another example. "Safety in numbers" is normally a smart rule. If all your friends are jumping off a bridge, it's probably because they know the water beneath is deep enough. If you stay with a crowd, you're less likely to get mugged than if you go off on your own. But on Facebook, everyone can suffer a privacy burn at the same time. That's what happened when News Feeds first came out; it's also what happened when some ill-behaved applications started using people's profile pictures without permission to show ads.

Facebook turns out to be a very effective tool not just for creating new social contexts, but for violating them, as well. The same Facebook servers that make it easy to send your friends messages also make it easy for them to copy and paste your words into an email. The same tools that make it easy to share an announcement with your whole network of college friends also make it easy to overshare with them. (That's what happened to Bono; one of the young women accidentally shared the photos with the entire city of New York.) The same easy profile browsing that lets you find new friends enables stalkers, employers, deans, and police officers to check up on you.

Making matters worse, the "safety in numbers" and "know your audience" rules of thumb are also partly responsible for Facebook's rapid growth. Remember that the biggest reason to be on Facebook is that your friends are there. The smiling face in your profile picture helps convince your friends that they're talking specifically to you, not to the anonymous masses. That reassuring counter—mine

says “347 friends”—is an indication of how much socializing you’d be missing out on if you walked away. Facebook recruits you into helping violate your friends’ privacy, just as it recruits them into helping violate yours.

Facebook, in other words, is a privacy virus. It targets new host organisms by tricking their natural privacy defense mechanisms into thinking it’s harmless. Once they trust it, Facebook uses them to infect others, spreading outwards from person to person in a social network. And everywhere it goes, people come down with exotic new privacy diseases.