

Privacy and Security

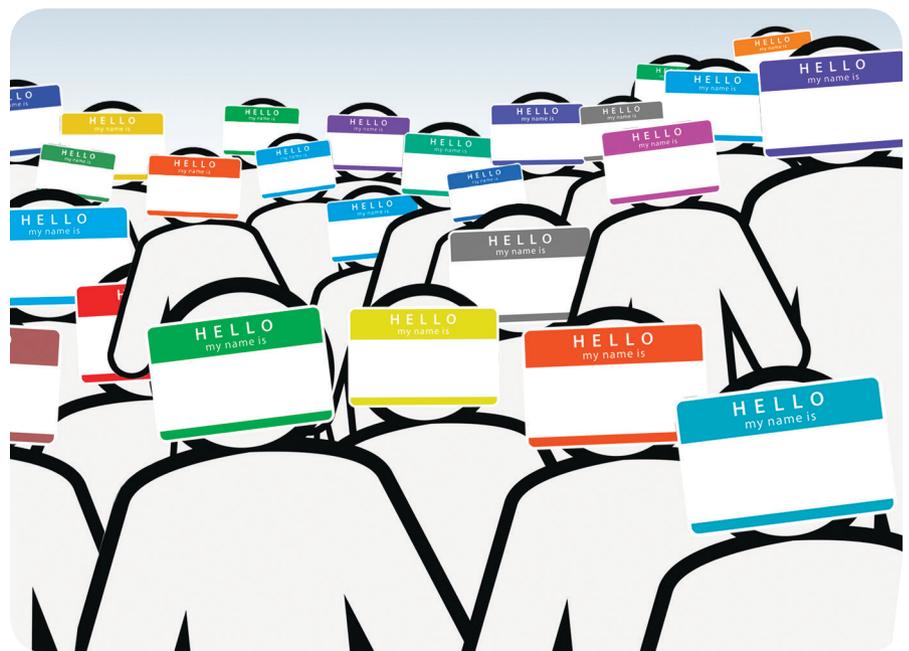
The Politics of “Real Names”

Power, context, and control in networked publics.

FACEBOOK'S TERMS OF service explicitly require its users to provide their “real names and information.” Indeed, the norm among many Facebook users is to provide a first and last name that appears to be genuine. Thus, when Google+ launched in the summer of 2011, it tried to emulate Facebook by requiring that new users provide similar credentials. Many early adopters responded by providing commonly used nicknames, pseudonyms, and stage names. Google, determined to ensure compliance, began expelling people who did not abide by the “real names” requirements. They ejected high-profile geeks, including Limor Fried and Blake Ross for failing to use their real names; they threatened to eject Violet Blue, a well-known sex educator and columnist.

The digerati responded with outrage, angry with Google for its totalitarian approach. The “nymwars,” as they were called, triggered a passionate debate among bloggers and journalists about the very essence of anonymity and pseudonymity.^{2,3,6} Under pressure, Google relented, restoring users accounts and trying to calm the storm without apologizing. Meanwhile, Google's chairman Eric Schmidt publicly explained the “real names” policy is important because Google Plus is intended to be an identity service.¹

While the furor over “real names” has subsided—and Google now supports pseudonymity—key questions about the role of identity, privacy, and



control remain. Why did people respond with outrage over Google while accepting Facebook? Do “real names” policies actually encourage the social dynamics that people assume they engender? Why did people talk about “real names” policies as a privacy issue? This column explores these issues, highlighting the challenges involved in designing socio-technical systems.

Facebook vs. Google: Norms, Values, and Enforcement

At Harvard, Facebook's launch signaled a safe, intimate alternative to the popular social network sites. People provided their names because they saw the site as an extension of campus life. As the site's

popularity grew, new users adopted the norms and practices of early adopters. The Facebook norms were seen as operating in stark contrast to MySpace, where people commonly used pseudonyms to address concerns about safety. Unlike MySpace, Facebook appeared secure and private.

As Facebook spread beyond college campuses, not all new users embraced the “real names” norm. During the course of my research, I found that late-teen adopters were far less likely to use their given name. Yet, although Facebook required compliance, it tended not to actively—or at least, publicly—enforce its policy.

Today, part of Facebook's astronomi-

cal value stems from the quality and quantity of information it has about its users. While it is unlikely that Mark Zuckerberg designed Facebook to be an identity service, that is what it has become. Google's competitive move is explicitly an identity play. Yet, rather than creating a value proposition in which users would naturally share their real names, they made it a requirement.

Larry Lessig argues that four forces regulate social systems: the market, the law, social norms, and technology or architecture.⁴ Social norms drove the "real names" culture of Facebook, but Google's approach was purely driven by the market and reinforced by corporate policies and technology. Their failure to create the conditions in which newcomers felt comfortable sharing their names—and their choice to restrict commonly used pseudonyms—resulted in a backlash. Rather than designing an ecosystem in which social norms worked to their favor, their choice to punish dissidents undermined any goodwill that early adopters had toward the service.

Implicit Assumptions about "Real Names"

Although some companies implement "real names" policies for business reasons, many designers believe such policies are necessary to encourage healthy interactions in online communities. Implicit is the notion that in "real life," people have to use their "real names" so why shouldn't they be required to do so online? Yet, how people use names in unmediated interactions is by no means similar to what happens online.⁵

When someone walks into a cafe, they do reveal certain aspects of themselves while obfuscating other aspects of their identity. Through their bodies, they disclose information about their gender, age, and race. Through fashion and body language, people convey information about their sexuality, socioeconomic status, religion, ethnicity, and tastes. This information is not always precise and, throughout history, people have gone a long way to obscure what is revealed. While people often possess documents in their wallets that convey their names, this is not how most people initiate interactions.

The practice of sharing one's name

Privacy is not about restricting information; it is about revealing appropriate information in a given context.

is embedded in rituals of relationship building. People do not share their names with every person they encounter. Rather, names are offered as an introductory gesture in specific situations to signal politeness and openness.

While the revelation of a person's name may link them to their family or signal information about their socioeconomic position, most names in a Western context provide little additional information beyond what is already conveyed through the presence of the individual. As such, they simply serve as an identifier for people to use when addressing one another. Online, the stakes are different.

Online, there are no bodies. By default, people are identified through IP addresses. Thus, it is common to lead with a textual identifier. In the days of Usenet and IRC, that identifier was typically a nickname or a handle, a username, or an email address. With Facebook and Google Plus, people are expected to use their names.

The power of search also shifts the dynamics. Although it is possible for wizards in Hogwarts to scream the equivalent of "grep" into the ether and uncover others' location, background information, and relationships, this is not something mere mortals can do in everyday life. Until the Internet arrived. Today, information about people can be easily accessed with just a few keystrokes. Through search, the curious can gain access to a plethora of information, often taken out of context. Without the Internet, inquiring about someone takes effort and provokes questions. Asking around often requires addressing a common response, "Why do you

want to know?" Yet, search engines empower the curious to obtain—and misinterpret—information without any social consequences. That shifts how people relate online.

Privacy and Names

Accountability is commonly raised as one of the reasons behind which people should provide identifiable information in online settings. When people prefer not to share their names, they are assumed to have something to hide. Many people claim people are better behaved and more "honest" when their identifying information is available. While there is no data that convincingly supports or refutes this, it is important to note that both Facebook and face-to-face settings continue to be rife with meanness and cruelty.

Even if we collectively value accountability, accountability is more than an avenue for punishment; accountability is about creating the social context in which people can negotiate the social conditions of appropriate behavior. Most social norms are regulated through incentive mechanisms, not punishment. Punishment—and, thus, the need to identify someone outside of the mediated context—is really a last-resort mechanism. The levers for accountability change by social context, but accountability is best when it is rooted in the exchange.

There are people who abuse other's trust, violate social norms, or purposefully obscure themselves in order to engage in misdeeds. This is not just a problem online. But most people who engage in lightweight obfuscation are not trying to deceive. Instead, they are trying to achieve privacy in public environments.

Wanting privacy is not akin to wanting to be a hermit. Just because someone wants to share information does not mean they want to give up on privacy. When people seek privacy, they are looking to have some form of control over a social situation. To achieve that control, people must have agency and they must have enough information to properly assess the social context. Privacy is not about restricting information; it is about revealing appropriate information in a given context.

People feel as though their privacy has been violated when their agency has

been undermined or when information about a particular social context has been obscured in ways that subvert people's ability to make an informed decision about what to reveal. This is why people feel so disempowered by technological moves where they feel as though they cannot properly manage the social situation.

In unmediated contexts, choosing when or how to reveal one's name allows people to meaningfully control a social situation. For example, when a barista asks a customer for her name, it is common for the customer to provide only her first name. There are also customers who provide a nickname or a fake name when asked for such information, particularly if their name is obscure, hard to pronounce, or overly identifiable. The customs involved in sharing one's name differ around the world and across different social contexts. In some settings, it is common to only provide one's last name (for example, "Mr. Smith"). In other settings, people identify themselves solely in relationship to another person (for example, "Bobby's father"). People interpret a social situation and share their name based on how comfortable they are and what they think is appropriate.

When people are expected to lead with their names, their power to control a social situation is undermined. Power shifts. The observer, armed with a search engine and identifiable information, has greater control over the social situation than the person presenting information about themselves. The loss of control is precisely why such situations feel so public. Yet, ironically, the sites that promise privacy and control are often those that demand users to reveal their names.

Who Is in Control?

Battles over identity, anonymity, pseudonymity, and "real names" are not over. New systems are regularly developed and users continue to struggle with how to navigate information disclosure. What is at stake is not simply a matter of technology; identity in online spaces is a complex interplay of design, business, and social issues. There is also no way to simply graft what people are doing online onto what they might do offline; networked technology shifts how people engage with one another.

Thus, it is important to move away from offline metaphors in order to address the complexity of people's mediated interactions.

The "real names" debate goes beyond identification technologies and economic interests. Regardless of the business implications, the issue of whether or not to mandate "real names" is fundamentally one of power and control. To what degree do designers want to hold power over their users versus empower them to develop social norms? To what degree do companies want to maintain control over their systems versus enable users to have control over their self-presentation and actions?

These are complex socio-technical questions with no clear technical or policy solution. Furthermore, even though design plays a significant role in shaping how people engage with new technologies, it is the interplay between a system and its users that determines how it will play out in the wild. Design decisions can inform social practices, but they cannot determine them. As with all complex systems, control is not in the hands of any individual actor—designer, user, engineer, or policymaker—but rather the product of the socio-technical ecosystem. Those who lack control within this ecosystem resist attempts by others to assert control. Thus, finding a stabilized solution requires engaging with the ecosystem as a whole. □

References

1. Banks, E. Eric Schmidt: If you don't want to use your real name, don't use Google+. *Mashable* (Aug. 28, 2011); <http://mashable.com/2011/08/28/google-plus-identity-service/>.
2. Dash, Anil. If your Website's full of a——, it's your fault. *A Blog About Making Culture* (July 20, 2011); <http://bitly.com/JAyktS>.
3. Fake, C. Anonymity and pseudonyms in social software. *Caterina.net* (July 26, 2011); <http://caterina.net/wp-archives/88>.
4. Lessig, L. *Code: And Other Laws of Cyberspace*. Basic Books, New York, 1999.
5. Madrigal, A. Why Facebook and Google's concept of 'real names' is revolutionary. *Atlantic Monthly*, (Aug. 5, 2011); <http://www.theatlantic.com/technology/archive/2011/08/why-facebook-and-googles-concept-of-real-names-is-revolutionary/243171/>.
6. Skud. Preliminary results of my survey of suspended Google+ accounts. *InfoTropism* (July 25, 2011); <http://infotrope.net/2011/07/25/preliminary-results-of-my-survey-of-suspended-google-accounts/>.

danah boyd (danah@danah.org) is a senior researcher at Microsoft Research, a research assistant professor in Media, Culture, and Communication at New York University, a visiting researcher at Harvard Law School, a fellow at Harvard's Berkman Center, and an adjunct associate professor at the University of New South Wales.

Copyright held by author.

Calendar of Events

August 17–19

International Conference on Security of Internet of Things, Amritapuri, India, Sponsored: SIGSAC, Contact: Rangan Venkat, Email: venkat@amrita.edu

August 21–24

Information Interaction in Context: 2012, Nijmegen, Netherlands, Contact: Kraaij Wessel, Email: wessel.kraaij@tno.nl

August 26–29

Advances in Social Networks Analysis and Mining 2012, Istanbul, Turkey, Sponsored: SIGMOD, Contact: Can Fazli, Email: canf@cs.bilkent.edu.tr

August 27–29

12th International Conference on Quality Software, Xi'an China, Contact: Zhou Xingshe, Email: zhousx@nwpu.edu.cn

August 28–31

Asia Pacific Conference on Computer Human Interaction, Matue-City, Shimane Japan, Sponsored: SIGCHI, Contact: Kentaro Go, Email: go@yamanashi.ac.jp

September 3–6

8th International ICST Conference on Security and Privacy in Communication Networks, Padua, Italy, Contact: Mauro Conti, Email: conti@di.uniroma1.it

September 4–6

24th International Teletraffic Congress, Krakow, Poland, Contact: Papir Zdziasaaw, Email: papir@kt.agh.edu.pl

September 4–7

ACM Symposium on Document Engineering, Paris, France, Sponsored: SIGWEB, Contact: Cyril Concolato, Email: cyril.concolato@enst.fr

September 6–8

The International Workshop on Internationalisation of Products and Systems, Bangalore, Kanatak India, Contact: Apala Lahiri Chavan, Email: apala@humanfactors.com