Harvard Business Review | Digital Article

Psychology

Why We're So Hypocritical About Online Privacy

by Tomas Chamorro-Premuzic and Nathalie Nahai

Why We're So Hypocritical About Online Privacy

by Tomas Chamorro-Premuzic and Nathalie Nahai

Published on HBR.org / May 01, 2017 / Reprint H03N00

Social psychologists have known for decades that the relationship between attitudes and behaviors is complex, if not weak. This is true online as well as offline. For example, though you may be irritated by the retargeting ads that follow you around the web, it probably hasn't changed your online shopping behavior. By the same token, the widespread anger and distrust reported by the general public when the Edward Snowden NSA saga erupted did not decrease internet use. In fact, it did not even increase the adoption rate of higher security settings on social media. In other words, even when people say they are concerned with online privacy, their concerns may not be strong

enough to drive digital abstinence. While more people are using VPNs, ad blockers, and tracking blockers to reclaim lost privacy, they're still in the minority.

Since you are reading this, we can only assume that you are at least somewhat worried about your online privacy. And yet there's a low probability that you take measures such as controlling the emails that people send you, removing cookies from your browser, regularly checking your computer for spyware, and deleting your browser history. Recent research suggests that even when consumers don't trust that their social media data is safe, they have no plans to protect it or opt out. However, intentions are typically weak predictors of subsequent behaviors. For instance, most people say they would take a pay cut in order to work less or do more interesting work, but very few actually do. So the big question is not what people allegedly plan to do about privacy, but what they actually do.

To address this question, a recent meta-analysis of 166 studies, including 75,269 participants of 34 countries, explored the so-called "privacy paradox," that is, the puzzling fact that people's concerns about privacy rarely appear to translate into protective behaviors. Contrary to previous studies, the findings of the meta-analysis revealed that individuals who are more concerned with and informed about privacy tend to use fewer online services, set stronger security settings, and disclose less personal information. However, when it comes to social media use, there is indeed a privacy paradox, as even individuals who express concerns behave quite carelessly, engaging in uncensored or inappropriate self-disclosure, making a great deal of their digital footprint public, and allowing a wide range of external apps to access their data. It has been estimated that nearly 40% of Facebook content is shared according to the (rather unsafe) default settings, and that privacy settings match users' expectations only 37% of the time. Thus, it appears

that no amount of privacy concerns will make social media users more cautious.

One of the possible explanations for the privacy paradox is *third person bias*, which suggests that even when people perceive potential risks in using social media, they somehow believe that those risks don't apply to themselves — just to others. This capacity for self-denial has been found in a wide range of risk-related activities, from drinking, to smoking, to having unprotected sex. It is not a lack of awareness of the risks associated with these activities that explains people's willingness to take those risks in the first place, but rather the illusion that those risks apply only to other people and not to ourselves.

Video Boards Neglect Cybersecurity at Their Companies' Peril
To view, please visit this article at HBR.org.

Another, more obvious explanation for the privacy paradox is a simple risk-reward assessment. Most of us would indeed prefer to feel safe and protected when we go online, but the perceived benefits of using free sites and disclosing personal information outweigh the perceived risks. As scientific studies have shown, most people use social networks to gratify fundamental psychological needs, such as the need to get along, construct and display their values and identity, and be entertained. If consumers were given the choice to pay for the free apps and online services they use in exchange for withholding all of their personal data, they would probably decline, preferring instead to pay *with* their personal data.

Because people's concerns about privacy don't seem to translate into behaviors to protect privacy, it is quite easy to envision a future in

which everything we do online becomes part of our public reputation. Our digital footprint can already be used to infer our deepest character traits; a 2013 study of 58,000 Facebook users (who volunteered for the study) was able to reliably predict sexual orientation, gender, race, age, religious and political views, level of intelligence, alcohol and cigarette use, drug use, and whether the volunteer's parents were separated. The researchers were also able to predict, to some degree, personality traits, such as extraversion, conscientiousness, openness, emotional stability, and agreeableness.

If that's what we can do already, is it really so hard to imagine a future in which our Uber ratings could be used to infer our likability or emotional intelligence, our Spotify and Netflix preferences to infer our curiosity and openness to experience, or our Amazon history to infer our impulsivity and conscientiousness? Even the words we say on Twitter, the things we like on Facebook, the websites we tend to visit, and the sound of our voices can be turned into a fairly detailed psychological profile, and the potential for trading this data is by no means confined to the world of marketing. The insurance, financial services, dating, and recruitment industries are all interested in the data, and few platforms would have launched or been funded if it weren't for the prospect of monetizing their users' personal data, which is the price we pay for anything that's free. Needless to say, there are many potential dangers (and ethical issues) associated with the proliferation of digital profiling, from hacking, to discrimination, to an Orwellian surveillance state. There's a big difference between what companies could and should know.

As one of us (Nathalie) has shown in a recent book on the psychology of online persuasion, although targeted data may have a positive effect on purchase intention, it can come with a hidden cost, particularly with more invasive practices. That cost is called *psychological reactance*,

which refers to the aversive emotional state we experience in response to perceived threats to our freedom and autonomy. It's this phenomenon that kicks in, for example, when we receive an off-base advertisement from a brand we don't know, don't trust, or have never bought from. Vendors and apps will need to constrain what they do with consumers' data, which means resisting the temptation to overuse it. For instance, if Facebook, Amazon, or Google overexploit the data they have, they may undermine consumer loyalty.

Perhaps the novelist Gabriel García Márquez was able to foresee the issue at the heart of the privacy debate today when he said: "All human beings have three lives: public, private, and secret." We have our public life, which is what we willingly do and share with others in a wide range of social settings. There is our private life, which we reluctantly give away in the hope that it is not fully revealed to the world or to those who shouldn't see it. Finally, there is our secret life, which, for now, can only be found offline. In fact, one may actually wonder: Is there really any such thing as a "secret" life anymore?

Tomas Chamorro-Premuzic is the Chief Innovation Officer at ManpowerGroup, a professor of business psychology at University College London and at Columbia University, co-founder of deepersignals.com, and an associate at Harvard's Entrepreneurial Finance Lab. He is the author of *Why Do So Many Incompetent Men Become Leaders? (and How to Fix It)*, upon which his TEDx talk was based. Find him on Twitter: @drtcp or at www.drtomas.com.

Nathalie Nahai is an international speaker and author of the best-selling book, Webs of Influence: The Psychology of Online Persuasion (Pearson). She lectures internationally on the digital application of behavioral sciences, has hosted Guardian podcasts, and contributes to national publications, TV and radio on the subject. Find her on Twitter @nathalienahai or at www.nathalienahai.com.

