THE CHRISTIAN SCIENCE MONITOR

Why you have the right to obscurity

Federal Trade Commissioner Julie Brill says that obscurity means that personal information isn't readily available to just anyone. In our age of aggressive data collection, she says safeguarding obscurity should be a key component of consumer protections.

By Evan Selinger, Columnist and Woodrow Hartzog, Contributor

April 15, 2015

Some people argue that the Digital Age has eviscerated obscurity. They say shifts in the technological and economic landscapes have forever changed society.

Their argument is that a tipping point has occurred; it's now too late to stop others from collecting, aggregating, and analyzing nearly every aspect of our data trail, and profiting from a steady stream of intrusive privacy invasions.

Federal Trade Commissioner Julie Brill insists the naysayers are wrong. Ms. Brill not only says there's ample evidence that people at home and abroad value obscurity, but she further contends that new domestic legislation should be enacted to provide consumers with the enhanced obscurity protections and other privacy protections that they deserve. We recently spoke with Brill about her obscurity agenda. Edited excerpts follow.

Selinger and Hartzog: *Your vision for how to best enhance consumer protections has a strong obscurity component. Since the term "obscurity" isn't widely used in legal and policy circles, let's begin with a definition and basic context. What does obscurity mean and why have you adopted the vocabulary?*

Brill: To understand what obscurity means, we first need to take a step back and talk about what privacy means. Louis Brandeis, the father of privacy in the modern era – as well as the father of the Federal Trade Commission – defined privacy as the "right to be let alone." The concept of privacy has clearly shifted in this "always on" age – where individuals cherish being connected, shopping online and through apps, and sharing with friends and colleagues through social networks, but believe that their online activities shouldn't be subject to invasive monitoring. While Brandeis' notion of seclusion is still clearly within the cluster of concepts that form our current understanding of privacy, I think the meaning of privacy now also includes an

individual's right to have some control over their online persona and destiny. Individuals want to be able to share with their friends and business associates on social media, shop online, and use connected devices, but they don't necessarily want all of these activities monitored, tracked, collected, and used by entities they do not know or with whom they have no relationship.

And this is where obscurity fits in. Obscurity means that personal information isn't readily available to just anyone. It doesn't mean that information is wiped out or even locked up; rather, it means that some combination of factors makes certain types of information relatively hard to find.

Obscurity has always been an important component of privacy. It is a helpful concept because it encapsulates how a broad range of social, economic, and technological changes affects norms and consumer expectations. In Brandeis' time, the technological change he was concerned about was the introduction of instant photography. Several scholars, including both of you, have discussed how many of our concerns about obscurity today center around digitized information and search tools that make it quick and cheap to do what was once expensive and slow – often prohibitively so.

But obscurity – or concern about the lack of obscurity – stems from more than just technological developments. Business models and economic forces can lead to information becoming less obscure. Brandeis was as concerned about the practices of intrusive journalists and newspapers as he was about the advent of instant photography. Several decades later, the introduction of widespread credit reporting raised concerns about the lack of obscurity.

After World War II, an increasingly interconnected national economy drove demand for widespread availability of information about individual consumers' character and creditworthiness – information that was once only available through personal references or a trip to a local courthouse.

Selinger and Hartzog: *What obscurity protections do you believe consumers are entitled to?*

Brill: Let's start with the obscurity protections provided under current law. Perhaps the clearest example under federal law is found in the Fair Credit Reporting Act (FCRA), which was enacted in 1970 to address increasing concerns in the 1950s and 1960s over the amount and type of sensitive information held by credit reporting agencies. The FCRA limits the amount of time that credit bureaus can report negative information about consumers in their credit reports. For example, the FCRA says that credit bureaus can't report information about unpaid debts, civil judgments, and a wide range of other "adverse" information if it is more than seven years old. In addition, bankruptcies have to vanish from credit reports after 10 years. Thus certain information is obsolete and irrelevant for credit reporting purposes and, by being taken out of credit reports, becomes much more obscure. The FCRA's obsolescence provisions reflect the judgment of Congress that negative information should not follow consumers around forever, and that consumers deserve a fresh start on their credit reports after a certain amount of time.

There are a couple of additional important aspects of the FCRA's obsolescence provisions. First, they are designed to operate without requiring consumers to take any action at all. When information gets too old, that's it – credit bureaus can't report it any longer. Second, these

obscurity provisions are only one facet of a larger framework of privacy protections within the FCRA. The law also gives consumers rights to access and correct information in their credit report, and sets standards for the accuracy and security of the information. All of these provisions work together to make the FCRA a comprehensive consumer protection law.

But the FCRA and its obscurity provisions aren't nearly enough to protect consumers adequately in the age of data brokers, people search firms, and other forms of data collection and use going on behind the scene that potentially invade privacy. For instance, data brokers and people search firms create profiles about individuals that contain information about their interests and activities – from both online and offline sources – and about such sensitive characteristics as their race, religion, political affiliations, and financial status. Consumers should have the chance to delete their people search profiles whenever they want, and should be given access and deletion rights – or in some circumstances correction rights – with respect to the profiles that data brokers have about them. Making sure that consumers have these choices is the right place to focus our attention as the discussion about broader obscurity protections unfolds.

Selinger and Hartzog: *How have debates about Europe's so-called "right to be forgotten" rule influenced your views on obscurity protections?*

Brill: The Court of Justice for the European Union's (CJEU) decision in Google Spain v. AEPD was momentous. It sparked a lot of debate among academics, the privacy and business communities, and elsewhere about what a right to be forgotten should mean for companies and consumers. As many commentators noted, the right to be forgotten label doesn't really fit the court's decision. The court instead focused on whether information returned in response to a search of an individual's name is relevant, adequate, and not excessive.

A few months after the CJEU's decision, I gave a speech in Vienna at an event attended by high level EU jurists and policy makers. I had thought a lot about the CJEU's decision, and decided to make it one of the touchstones of my speech. I noted that I agree with commentators who argued that a better label for the CJEU's decision was a "right to relevancy" or "right to preserve obscurity." Then I posed some questions about how search engines should decide when a piece of information is no longer relevant, how to determine whether a search relates to an individual in his or her role in public life, and how the decision might be applied and enforced outside the EU. I also drew some parallels between the CJEU's decision and pockets of US law, including FTC enforcement actions, that include requirements to keep information obscure, or at least allow consumers to do so.

But the parallels between the CJEU decision and some of the obscurity provisions currently contained in US law only go so far. Currently, obscurity protections in the US are targeted, either through legislation that outlines clear requirements, or through enforcement orders that apply to specific companies that engaged in activities that were "deceptive" or "unfair."

I think we need to expand obscurity protections here in the US, through enactment of legislation that would require data brokers to provide greater protections to consumers, and through more comprehensive privacy legislation.

Selinger and Hartzog: *People often say the right to be forgotten would never work in the US. Do you share the same pessimism?*

Brill: I am optimistic that we can infuse a workable right of obscurity into our privacy framework here in the United States. Indeed, the right of obscurity should become a part of the current discussion among policymakers and a wide variety of stakeholders about needed improvements to our privacy framework here in the US. However, I don't believe a broad EU-style right to be forgotten will be included in these discussions, because the further reaches of a broad right to be forgotten modeled on the CJEU's decision would raise serious questions under the First Amendment here in the US.

For that reason alone, I prefer to focus on somewhat more targeted approaches to a right of obscurity that could work here and provided much needed additional protections to individuals.

As I mentioned, we already have elements of a right to be obscure here in the US. In addition to the FCRA, we have another example in California's recently enacted "eraser button" law that requires operators of online services to allow minors to remove content that they posted on the service.

I have long called for consumers to be given tools to enhance their obscurity in other appropriate circumstances. Both the White House and my colleagues at the Federal Trade Commission have adopted many of my proposals. In a report on data brokers, the FTC recommended legislation that would allow individuals to opt out of data brokers sharing their information for marketing purposes. The FTC also recommended legislation that would allow individuals to tell a people search firm not to return results about them in response to searches of their names. In my own statement about FTC's data broker report, I called for legislation to go further by requiring data brokers to be accountable for the ecosystem they create. Many of these recommendations have now been included in a bill introduced by Senators Markey, Blumenthal, Whitehouse, and Franken. These recommendations provide a workable model for the US, as they are well tailored for specific, commercial settings.

Additionally, there are steps that data brokers can take right now to give consumers some of these tools. They should devote more resources to designing intuitive portals that allow consumers to enhance obscurity and control their privacy.

Selinger and Hartzog: *The FTC is the most central privacy regulator in the US. Much of the agency's power comes from Section 5 of the FTC Act, which broadly prohibits unfair and deceptive trade practices. Can the agency enhance obscurity protections under Section 5? Or does it need an additional grant of authority for optimal obscurity protection?*

Brill: The Federal Trade Commission's enforcement efforts play a role in enhancing obscurity protections. However, in the absence of specific legislative requirements like those contained in a data broker law, a federal eraser button law, or baseline privacy legislation, the Commission is limited to using its authority under current law in this area. In addition to its ability to enforce the provisions of the FCRA, the Commission has authority under Section 5 of the FTC Act to prohibit "unfair" or "deceptive practices. Because the Commission's Section 5 authority is broad

and remedial, the Commission has been able to require companies to allow consumers to delete or suppress information about themselves in some circumstances.

For example, in our settlement with Facebook, we required Facebook to ensure that information is actually deleted or rendered inaccessible within 30 days after a consumer marks the information for deletion or terminates her account. This provision in the Facebook order stems from the allegation in our complaint that Facebook allowed third parties access to content from consumers' accounts even after consumers deactivated or deleted their accounts.

And in our action against US Search, a people search firm, the Commission prohibited US Search from misrepresenting the extent to which its opt out removed publicly available information from searches on consumers' names, as well as how long the opt out would last. Again, that order provision is directly tied to our allegation that US Search deceived consumers about its opt out because there were several ways to uncover information about consumers even after they opted out.

These enforcement actions are important, as they make clear that companies must live up to their representations about the extent to which a company discloses (or deletes) sensitive, personal information about consumers.

Because our ability to enforce appropriate levels of obscurity is limited by current law, I believe Congress should adopt appropriate legislation that would provide consumers with better tools – tools that are robust, intuitive and interactive – to exercise a right of obscurity, and should give the FTC the ability to enforce these rights.

Evan Selinger is an associate professor of philosophy at Rochester Institute of Technology. Follow him on Twitter @EvanSelinger.

Woodrow Hartzog is an associate professor at Samford University's Cumberland School of Law. Follow him on Twitter @Hartzog.

http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0415/Why-you-have-the-right-to-obscurity?cmpid=TW