Efforts to Reform Online Identity Toil On

July 2, 2012

I have memorized five Internet passwords. Each contains a different mix of lower-case and capital letters, symbols, and numbers. One is especially long: my favorite line of poetry (with underscores replacing spaces).

A recent *New York Times* article [1] bemoaned the “mind-boggling array of personal codes squirreled away in computer files, scribbled on Post-it notes or simply lost in the ether.” Even my own unusually obsessive, security-conscious approach doesn’t save me from frequently resetting arbitrary passwords I can’t remember.

The password is a relic: a dated method of authentication of the same kind that governs children’s club houses. It is a key example of the inelegance with which we handle identity on the Internet today.

The Internet has become increasingly sophisticated and central to our lives, but some aspects lag behind. The password jungle is one symptom. Another is the fact that I can’t still can’t notarize a document or renew my driver’s license without waiting in long line across town.

For more than a decade, technologists and policy wonks have dreamed of better ways of handling identity online. Many have settled on a state that resembles a digital key ring – with each key revealing various amounts and different kinds of information about me. For example, I might have one identity for my hobbies and games (unverified by any authority and unrelated to my legal name, of course) and another identity for financial transactions and government services (much more highly verified). I would choose who I trust to keep and present my keys when I needed to use them. Gone would be my maze of usernames and passwords.

Obviously this idea has yet to catch on. However, a small office within the federal government is hoping to help push norms forward.

An Ambitious Government Strategy

Last year, the Obama Administration released a strategy called the National Strategy for Trusted Identities in Cyberspace (NSTIC) [2]. NSTIC is a federal strategy document: a roadmap for reforming how we present identities on the Internet. Jeremy Grant, the Senior Executive of the project describes NSTIC as “a bit of a policy experiment.” It’s not a statute or regulation, but an attempt at leading the private sector to produce and use new technologies, with new policies.

The primary vision of NSTIC is this:

Individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.

In more concrete terms, NSTIC aims toward a world where we use *fewer* online credentials across different sites and services, departing from the redundancy of today’s site-by-site accounts. These solutions might be installed in a browser, handled by a trusted Internet service (like an OpenID provider), chipped into a mobile phone, or resemble traditional ID cards, depending on the use case.

This might seem creepy at first glance. However, if properly achieved, the NSTIC vision could improve security and privacy for everyone. Consider that when you create a new account for each individual blogging service, newspaper, merchant, and social network you come across, you are casting your personal information to the wind. You subject your personal data to the diverse practices of numerous companies and increase the risk of your data being breached. However, by using fewer, secure identities, you can more selectively share information and potentially even

revoke a companies' access if you change your mind.

Going too far down this road invites new problems. Over-centralizing identity information might create a honey pot for hackers and identity thieves. The goal, then, is a balance somewhere in between. NSTIC ultimately has the right idea: *fewer* (not one!) interoperable identities users can choose between as they deem appropriate. Some identities would require special verification and proofing to obtain (e.g., those that would be associated with health or financial services). Many sites would require no identity assertions at all, of course, preserving space for online anonymity.

NSTIC at its core is a correct—albeit ambitious—picture of the sort of infrastructure we should want for the Internet. The government is not *creating* a new identity system or hosting the most of the credentials. Instead, it's trying to spur private companies, innovators, and academics to create an ecosystem that's useful to everyone.

Much difficult work remains to be done, though. And there are dangers that must be avoided.

The Hard Work Begins

Achieving the NSTIC vision won't be easy. The idea that we should be able to use identities across websites and services presupposes that everyone is talking the same language and agrees to abide by some shared policies. These shared understandings also underpin more "trustworthy" identities that open the doors for more sensitive online transactions. We've seen great success from Internet standards bodies in the past, but this effort is still novel in many ways.

The first step is to organize the conversation and set some ground rules. The National Institute of Standards and Technology (NIST), the agency overseeing NSTIC, recently produced a preliminary charter [3] and will form a "steering group" led by the private sector that works with the federal government to support NSTIC. Happily, privacy groups and advocates have a dedicated place at the table.

The work will soon shift to this primarily private forum, and then the real work begins. As the NSTIC National Program Office recently posted [4] on its blog:

While NSTIC is a government-initiated strategy, at the end of the day it will depend upon participation from key stakeholders like you to craft a framework for identity solutions that can replace passwords, allow individuals to prove online that they are who they claim to be, and enhance privacy. The Steering Group will be the most important forum for stakeholders to convene and collaborate on solutions to enable the Identity Ecosystem.

It will be important for privacy advocates to engage. While many details and goals remain vague, the process could be an important one. Any effort to tinker with how we identify and authenticate online—even with the best of intentions—could negatively impact privacy if not carefully designed. If designed wrong, a new identity regime could result in more tracking by companies providing the identity services. If designed correctly, we could all enjoy more secure, convenient, and private online interactions.

Only time will tell.

In the meantime, good luck remembering those passwords.

Copyright © 2013 by Center for Democracy & Technology.
The original text on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL: https://cdt.org/blogs/aaron-brauer-rieke/0207efforts-reform-online-identity-toil

Links:

[1] http://www.nytimes.com/2012/06/24/fashion/computer-passwords-grow-ever-more-complicated.html?pagewanted=all
[2] http://www.nist.gov/nstic/
[3] http://www.nist.gov/nstic/notices.html
[4] http://nstic.blogs.govdelivery.com/