Daniel E. Geer, Jr.
In-Q-Tel

Identity

Freedom requires accountability. Accountability requires authorization. Authorization requires authentication. Authentication requires identity. The logic seems inescapable or, at the very least, the burden of proof rests with those who would declaim an alternate construction.

But what is identity? Do we yet have an actionable, consensus definition? No, as of yet we do not. Perhaps we are closer than we were last year? Well, identity is a tough problem in the spirit of John Foster Dulles: "The measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year."

The nuances of identity are many. Suppose you are the decision maker in charge. If your policy goal is order, then you will seek unavoidable accountability via unarguable attribution of actions to identities—meaning undeniable identifiers tracked as such. If your policy goal is safety, then you will seek maximum privacy via making an ever greater fraction of interactions uncorrelatable. Of maybe I have those two exactly backwards; maybe safety is what location tracking a uniquely identifiable mobile phone is all about while order is when code is law.

Questions present themselves:

1. What can we do about uniqueness without resorting to simply numbering everything (including us)?
2. Who owns an identity?
3. Is a name simply a container for a set of authorities?
4. Which methods for identification scale?

It would seem that if a name is, in fact, universal and permanent, then that name is a thing of value. For some years now there has been this drumbeat from the cypherpunk wing that reputation is all that matters and that a name is merely a container for reputation, or, to put it differently, until a name is valuable it won't be protectable. And now whole industries embrace the idea. You see this in many of the arguments for who ought rightfully to issue and clear digital cash. You see this in examples where laissez-faire choice of names is shown to be harmful (and not just in the case of typosquatting).

You see it in the world of phishing and those who automate the name collection on which it depends. You see this where an enumeration of names, such as a listing of a brokerage's customers, is certainly not "information that wants to be free," which sounds like a working definition of property. ICANN more or less does nothing else than adjudicate the ownership of names (all the while its unbounded proliferation of top-level domains has been perhaps the most criminogenic policy decision ever made, unless you count opaquifying the beneficial owners of domains). Every marketing department in the world sings the theme song of marketing success: "name it and claim it." In short, names must be owned, but if you need a specialty land court, don't you need a specialty name court?

This is not to say that one would like pervasive, universal accountability, per se, but the only reason a free society works is that you can pretty much do anything with the caveat that if you screw up badly you'll be found out and made to pay. Accountability is a log processing task plus a test of will—if there are identities.

Thus, the paradox of identity: To protect liberty we must not confuse ourselves with side effects, e.g., confusing anonymity's technically assured privacy—a cheap substitute for a civilization-sized assured devotion to privacy rights—with the main goal of identity, which is accountability as the bulwark of liberty. Identity that can be relied upon is the sine qua non of accountability and thus with the preservation of liberty. Trust, as economic historians and social economists have long assured us, is efficient if and only if that trust is warranted and, for when it is not, effective recourse is available. Classic full-trust examples such as the diamond merchants of NYC's jewelry district illustrate the point, or, to go further back, the Hanseatic League.

For all of security, keeping honest people honest is a high goal, one that is economically and technically feasible. Keeping dishonest

Digital Object Identifier 10.1109/MSEC.2022.3173817
Date of current version: 11 July 2022

continued on p. 71

 Copublished by the IEEE Computer and Reliability Societies

 continued from p. 72

people honest is far harder, more like military occupation than policing, and will not be a net economic enabler—quite the opposite.

So to repeat, freedom requires accountability. Accountability requires authorization. Authorization requires authentication. Authentication requires identity. The logic seems inescapable or, at the very least, the burden of proof clearly rests with those who would declaim an alternate construction. Do not forget the sociopolitical reality that when a risk cannot be managed, whether for technical reasons or for reasons of apathy and unresolve, that the risk will be assigned, at best as a legal liability for some party designated by legislative fiat. Sometimes this is a long-term net good as Regulation Z of the Truth in Lending Act may be said to have done in capping credit-card loss limits by assigning the risk of forgery to the card associations, but most times risk assignment is an economic distortion and a net tax on the weak or on wealth creation as it is a tax on productivity growth. We leave that debate to another time.

There are certainly examples of a name being but a container. Put operationally, would you like a few containers that are distinct from each other? Do you use your real name with each and every online merchant you deal with, or do you use a different name with each? You've been told to never use the same password at multiple sites, but isn't that picayune risk reduction if you have the same name at every site? Are you risk averse enough to never order customized computing gear assembled offshore under a name others know?

There's more, of course, but it all leads in the same direction; identity is complex, and the benefits of complexity do not come cheaply, or to be more precise, we know that optimality and efficiency work counter to robustness and resilience. We know that complexity hides interdependence, and unacknowledged interdependence is the source of black swan events. We know that the benefits of digitalization are not transitive, but the risks are. Identity, naming, and the functions we must put around it are a prime example of these truths.

Will we have this problem to deal with a year from now? ■

Daniel E. Geer, Jr. is a Senior Fellow at In-Q-Tel, USA. His collected works are available at http://geer.tinho.net/pubs. Contact him at dan@geer.org.

Digital Object Identifier 10.1109/MSEC.2022.3183371