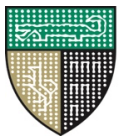

Information Society Project
Yale Law School

DIGITAL FUTURE WHITEPAPER SERIES

Identity, Thy Name Is Gordian

Dan Geer

May 2021

Contents

Identity, Thy Name Is Gordian

I. Welcome to the Internet

The issue of identity is passing unignorable. The nature of the web—that everything and everyone is equidistant—erases the inherited intuitions of the public at large even if the public understands that when you cannot tell a computer from a person, you can drop the distinction.

Identity in a connected world is certainly different than in the village where, to a first approximation, you know everyone and everyone knows you—"you" being both your physical manifestation plus your history and kinship. Literature and catwalks alike are overrun with folks who claim that their real life only began when they moved to some place where nobody knew who they were and, better still, someplace big enough that the odds of seeing the same person twice are zero unless it was intentional. They call this freedom.

So welcome to the Internet. You don't have to be told that things here are seldom as they seem, that milk often masquerades as cream. What, then, does identity mean in, on, around, or through the Internet? As the easiest way out, one might take Humpty Dumpty's position, that "When I use a word, it means just what I choose it to mean—neither more nor less." But that is the equivocation of a wannabe petty tyrant.

In the meantime, the Internet can be said to have an opinion given that the Internet does, in fact, have a dog in the fight. All the mechanisms that keep the myriad parts of the Internet running stand on the triad of authentication, authorization, and accountability. To be precise, authentication is "who are you?" Authorization is "what are you permitted?" And accountability is "what did you do?" That triad predates the Internet and hasn't lost meaning, but the setting has lost meaning, and if you are going to plead for new understandings of the triad's components, you better be able to plainly say what problem you are trying to solve.

II. Core Components

Let's start at the beginning with authentication. As it stands today, but perhaps not much longer, authentication begins with a claim and is followed by an endorsement. As with every security gatekeeping function, the times when the gatekeeper says "No" are ever so much more important than the times when it says "Yes." A claim of the form "The name is Bond, James Bond" can either be accepted as is or it can be met with the rejoinder "Prove it." Such proving is recursive insofar as the proof that Mr. Bond offers you relies on your trust in some higher authority—if you trust M, then it follows that you accept M's endorsement that this man is James Bond. That is recursive: your trust in M is based on an endorsement of M by M's higher authority, and so forth. But that has to stop somewhere. In so many words, in an authentication setting, a claim of identity calls for deductive reasoning: if you trust M and M says that he is James Bond, then he is James Bond. But trust needs what in the trade is called a "trust anchor," something which functions like an axiom in mathematics. That's true even for the semi-anarchist versions of non-hierarchical hierarchy.

The power, if you want to talk about power, of the endorser is clerical and discretionary, to intake and retain names and to vouch for them when asked, and, of course, to cancel such a registration (which we'll attend to shortly). There are myriad technical details, which include what is the nature of an acceptable name, how to disambiguate identical names amongst different entities, and name changes if such are allowed. A name, in short, is context-dependent. When a name is random or otherwise meaningless, such as a "universal unique identifier" (UUID) generated for an embedded device, the rules will be different and may not allow for name changes at all.[1] Once a name is well enough known, there's no competing with it anyhow (Marilyn Monroe versus Norma Jeane Mortenson). A name is a gift from others, and changing a name is just sending the gift back. (Incidentally, if you think cybersecurity is hard, naming is harder.)

To illustrate how names and identity interact, consider the way in which an endorser endorses an identity. In the typical digital space, there is a pairing of a name and a cryptographic key. A person (or other entity) claims a name and proves they have a secret that only the rightful person would rightfully know. Amongst other things, this means that if the cryptographic key is stolen, the thief will have just as endorsable a claim to the

name as the original assignee. Identity theft is poorly named insofar as an identity is not stolen but cloned; the victim still has his or her identity-proving secrets, just not exclusively. Which brings us to a bit of a philosophical question: Do we prefer name-centric authentication or key-centric authentication?

In name-centric authentication, the name is the identity, and the key is an attribute of the name.[2] In key-centric authentication, the key is the identity, and the name is an attribute of the key. Does this key belong to Dan or does "Dan" belong to this key? Which one is the modifier and which the modified? Key-centric favors the bearer world (think Bitcoin). Name-centric favors the book-entry world (think your state's Office of Vital Records).[3] As with all of cybersecurity engineering, part of our job is to pick what failure modes are tolerable, including here.

III. Five Questions About Identity

Any identity system that purports to be universal or, which is more, at once both permanent and location (context) independent, is either brilliant or insane. Consider this to be the first question I raise, namely:

1. *What can we do about uniqueness without resorting to simply numbering everything (including us)?*

It is and will remain difficult to reconcile the desirable properties of non-repudiability and universality, to make a digitally-signed statement mean something evidentiary while at the same time having the name of the signer remain context free. Perhaps that explains the difficulty in thoroughgoingly adopting X.509 public key infrastructure systems inasmuch as the rigors of stranger-to-stranger introduction, which is the paragon of universality, produce more complexity than we can economically handle.[4] The debate between the name-centric and the key-centric styles of authentication is an argument over what it is that is sufficiently durable to be the primary identity and leaving the other, whether it is a name or a key, as a secondary data label. Those of you who are designers are facing a hard tradeoff:

Holding risk constant, the longer lived a name, the less informative it can be, while the more available the name is, the less dynamism it can support.

The second question I might raise about identity is this:

2. *Who owns an identity?*

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 on the cypherpunk fringe 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).[5] 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 traders, is certainly not "information that wants to be free," which sounds to me to be a working definition of property. ICANN (the International Corporation for Assigned Names and Numbers) 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. 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?

The third question is this:

3. *Is it possible to disencumber identity with biometry?*

It is already technically feasible to take attendance in a room without resorting to circulating a notepad and a ballpoint. Facial recognition, voiceprints, sniffing your microbiome out of the air, etc., make the 2-tuple of name and key into the 3-tuple of name, biometry, and key. Ron Rivest predicted twenty years ago that technologic advance would soon convert identity from being an assertion ("My name is Dan") to being an

observable ("Sensors confirm that this is Dan").[6] To that point, the claim of a name and the endorsement thereof are no longer a mechanism governed by policy but rather a received truth. From machines. This changes much; ask any pedestrian in Xinjiang.[7]

The fourth relates to the interaction of identity and permission:

4. *Is a name but a marker for authority?*

Authorization annotates an authenticated name with enumerated powers, much like United States is the name and the Constitution enumerates the powers of that name. Sometimes a name is that of a role and/or an honorific ("Officer," "Doctor," "Rabbi," "Barrister," etc.), that is to say one can address a person by the name of the role they play—the authorization being inherent in the role which, of course, to work must already be a common understanding amongst all the players. Authorization in the form of an ID card of any sort is at this margin between identity and permission. Merging authorizations onto the assertion of identity is a commonplace necessity, but there is an odd "gotcha" in the digital (computational) space: the irreducible vulnerability of any permission system to Denial of Service (DoS) resource consumption attacks is proportional to the amount of computation that a system must expend before it can make its authorization decision.[8] Ever finer-grained authorization decisions grow increasingly more complex, and the denier of service can call upon you to calculate them over and over. In that sense, authentication decisions, being as they are permanently simpler than authorization decisions, have a durable performance advantage.[9]

The fifth question is the biggest of all:

5. *Will our methods for identification scale?*

The desire for permanent, universal electronic identity is driven by the accumulating demands for access control in a complexifying world. While it was once an insight, it is now received truth that complexity is the chief enemy of security. If you look at the access control task, it is a matrix.[10] The rows are requestors, and the columns are objects of their desire. Linear growth in either or both means geometric growth in the number of table entries in that matrix. Sure, you can cut down the number of rows through role-based collective nouns and you can cut down the number of columns through cleverly crafted

policies for authority delegation (inheritance), but the natural path is that of geometric growth in the matrix.

If there is a finite lower bound on the cost of maintaining a check box in such a matrix, then the total cost of access control rises faster than the growth of the corporation either in size or assets. Any cost that rises faster than linear with growth cannot and will not stand indefinitely. Accountability is the only answer to the scalability defects of access control.

Accountability scales linearly in total corporate workload, not geometrically in total corporate assets, but only if authentication is present. Without a sense of "who," there can be no sense in sentences like "who did what and to whom." When the geometric scaling of access control reaches its eventual resource exhaustion event, accountability, the third leg of the triad, stands ready. 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 will be found out and made to pay. Accountability is a log processing task plus a test of will.

IV. The Problem Is Choice

Where does this leave us, thus far, with identity?

- It leaves us with identity as a creature of context.
- It leaves us with a tilt away from access control and towards accountability over time, accelerated wherever perimeters are dissolving.
- It leaves us with biometry as a tool of identity confirmation and poised to supplant identity assertion.
- It leaves us with any improvement in the value proposition for identity inevitably creating property rights questions in proportion to the increasing value of those names.

So, if choosing complexity inevitably means accountability standing on authorization standing on authentication, then we have the setting for a hard choice: Do you surveil people or do you surveil data? The connection to identity and the management thereof is

this: If we have to yield to the realities of a location independent, globalized world where "inside" and "outside" are a fiction, then we must be able to preempt threats based on intelligence we can believe in, meaning based in turn on surveillance. Our choice is whether to focus that surveillance on people or on data.

To focus on data is a critical question of liberty and facility, and must be sought to the extent possible ("possible" in the sense that politics is the art of the possible). We can focus our surveillance on data and yet still have personal accountability but only on the condition that identity markers associated with a data-oriented record are believable in and of themselves, i.e., that when necessary the activity stream of a person can be reconstructed from the activity stream of a datum. If identity is not up to this, we will inevitably surveil the activity stream of the person as our primary focus, a path that ends with a global despot.[11]

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

V. The Calculus of Identity

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.[12] We leave that debate to another time.

Is the Ship Too Big to Steer?

Are we at a "hinge of history?" When you are in the knee of a curve, you can't be reasonably expected to see that you are until you are past that knee and are on the genuinely exponential upslope. Is the eternal government vulnerability to regulatory capture being inexorably supplanted by technology capture—where in regulatory capture the regulatory agencies come to be dominated by the sheer mass of those industries they are charged with regulating, but in technology capture the regulatory agencies come to be dominated by the sheer momentum of technologic change (momentum = mass * velocity)? Is this the basic dilemma for those with a clear-thinking concern for where technologic interdependence leads, the dilemma being that you can't steer what you won't embrace? Does that make it suspicious, as in making you a person of interest, if you choose to opt out of having an online identity? Does not the matter of identity demonstrate once more that all security technology is dual use? There are so many aspects to this that this short essay is but another drop in the bucket of all that has been written about identity.

What some call self-determination, others call privacy, as merged in the words of Eric Hughes: "the power to selectively reveal oneself to the world."[13] If the data harvest of an interconnected, interdependent world kills both privacy as impossible-to-observe and privacy as impossible-to-identify, then what might be an alternative?[14] If you are an optimist or an apparatchik, then your answer will tend toward rules of procedure administered by a government you trust or control. If you are a pessimist or a

hacker/maker, then your answer will tend toward the operational, and your definition of a state of self-determinative identity will be mine: the effective capacity to misrepresent yourself.

Misrepresentation is using disinformation to frustrate data fusion on the part of whomever it is that is watching you. Misrepresentation means paying your therapist in cash under an assumed name. Misrepresentation means arming yourself not at Walmart but in living rooms. Misrepresentation means swapping affinity cards at random with like-minded folks. Misrepresentation means keeping an inventory of misconfigured webservers to proxy through. Misrepresentation means putting a motor-generator between you and the Smart Grid. Misrepresentation means using Tor for no reason at all. Misrepresentation means hiding in plain sight when there is nowhere else to hide. Misrepresentation means having not one digital identity that you cherish, burnish, and protect, but having as many as you can. The Realpolitik of the Internet: Your identity is not a question unless you work to make it be.

As we all know, some identities are both unique and decoupled from the physical world. Consider Satoshi Nakamoto, the purported inventor of Bitcoin. Does s/he exist? Does it matter? Consider Q, the purported insider from whom Q-Anon has grown up. Does s/he exist? Does it matter? For every algorithm that passes the Turing Test and has a name, how would you describe the algorithm's name if it claims one? Does it matter?

Those are certainly examples of a name being but a container. Put differently, 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?

If you've looked, then you know that it is has become pervasive for the beneficial owner of a domain name to be hidden from query on what are claimed to be privacy grounds. While it is well-considered U.S. law (FinCEN) that a bank "must establish and maintain written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customer," it is obvious that the average American will interact with two orders of magnitude more opaquely owned domains than with banks.[15]

VI. The Granularity of Identity

A little bit of history: When e-commerce began, all the inventors spontaneously came to a common conclusion—their systems needed to ensure that merchants would not know how you paid, only that you had, while banks would not know what you had bought, only that you had. Money would change hands but there would be no correlation (under your name) of how much you bought and of what at what price. Your name would be present all over, but there would be no data fusion of payment source and bought object.

Across the board, early designs had four parties—you, your bank, the merchant, and the merchant's bank. This design failed completely because the public didn't like it. You know why the public didn't like it? Because it made returning merchandise hard. The public likes to be able to trivially return merchandise, and all those little e-commerce companies either switched from the 4-way model to the 3-way model you know today, or they died. And now what you buy is an open book, as are you, if you have the same name everywhere you go. A container for reputation, are we?

But what about "things" that are nameless?[16] That's an important, and quickly growing, fraction of network-reachable devices, especially now that device cost is no barrier to deployment. Assuming that myriad, nameless devices will need to be able to cryptographically protect their messages, where is the key for that looked up? Will each device have one of its own? Will we not bother with keys at all and trust that the internal firewalls are resilient to lax operation? Perhaps especially interesting, what would a name mean when the end user has a half-dozen devices that mutually self-synchronize?

It's a policy question whether we should require resolvable names for some classes of services. At present, name resolution is the double-entry bookkeeping of the Internet (another endorser scenario where you claim that this name and address pair are connected, and I verify your claim with third parties neither of us control).

In the absence of names, how do you know to whom you are connected? Is a (nameless) address baked into a device and, if so, baked into what exactly? Does a software updating engine reach out to devices that have only a network address and no name? Does an endpoint that is asked to accept a pushed update have a source-name to check? Do we

need a two-class liability regime and/or duty for checkable name-to-address pairs versus unnamed addresses? Either way, is the key-management job going to be harder or easier absent names?[17]

For some of this, we are at the last exit before the toll road. The choices to be made will be expensive to later reverse in either dollars or clock ticks. Momentum says that soon, the majority of Internet endpoints will not be describable by name or discoverable by scanning. Another layer of indirection will, as ever, solve some problems and create others. Provenance and forensics will all but surely be affected in difficulty-enhancing ways. And we will wish for names that would just sit still.

There's more, of course, but it all leads in the same direction; 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. Naming and the functions we must put around it are a prime example of these truths.

References

---

[1] *Editors' note:* A UUID, or universally unique identifier, is a unique 128-bit number that is used for identification in software systems. *See* Nick Steele, *Breaking Down UUIDS*, DUO (June 21, 2019), https://duo.com/labs/tech-notes/breaking-down-uuids.

[2] *Editors' note:* A key in cryptography is a piece of information, a number that controls the mathematical algorithm used to encode or decode (e.g., hide or reveal) plaintext to or from encrypted form.

[3] *See* Carl Ellison, CyberCash Inc., Perry Metzger, Piermont Information Systems, Key-Centric PKI, Presentation at the USENIX Workshop on Electronic Commerce (1998), http://static.usenix.org/publications/library/proceedings/ec98/pki.html; Warwick Ford, Verisign, & Steve Kent, CyberTrust Solutions, Name-Centric PKI, Presentation at the USENIX Workshop on Electronic Commerce (1998), http://static.usenix.org/publications/library/proceedings/ec98/pki.html.

[4] *Editors' note:* X.509 public key infrastructure is an ITU standard that defines the format of public key certificates, which are variously used in networking protocols to verify identities by verifying that a distant party controls the cryptographic key formally associated with the claimed identity.

[5] *Editors' note:* The act of "typosquatting" consists of opportunistically capturing a user who inadvertently misspells the name of some network resource, such as hosting malicious content on a website with a similar but misspelled URL. An example might be using the URL "isp.jale.edu" (with a j) to attack a user who originally intended to visit "isp.yale.edu."

[6] This point was made personally and informally to the author, but is no doubt echoed through his scholarship. *See Ronald L. Rivest: Publications & Talks*, CSAIL MIT (last accessed Apr. 27, 2021), http://people.csail.mit.edu/rivest/pubs.html.

[7] *See* Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

[8] *Editors' note:* A distributed denial-of-service (DDoS) attack typically consists of overwhelming a server of some sort with an avalanche of syntactically legitimate requests so as to make the server unable to respond to normal requests, as when thousands of remotely controlled computers are caused to visit a webpage at the same time causing it to crash; unintuitively perhaps, but the more resource intensive authorization decisions are, the more susceptible such servers are to these types of attacks. *See* Dan Geer, *Unintended Side Effects in Security*, FIN. SERVS. INFO. SHARING & ANALYSIS CTR. (Apr. 2001), transcript available at http://geer.tinho.net/geer.fsisac.25iv01b.txt. Note that DDoS attacks are available as a service and cheap to buy. *See* Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFF. (Apr. 26, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021.

[9] For those readers actually in charge of an authentication cum authorization system, you should understand your perimeter to be the reach of your entitlements, the scope of where your authorization controls actually work. That's your real perimeter, not what might be written in legal boilerplate.

[10] *See* Vincent C. Hu, David F. Ferraiolo & D. Rick Kuhn, *Assessment of*

Access Control Systems, NAT'L INST. STANDARDS AND TECH. (Sept. 2006), https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf (defining an access control matrix as a "table in which each row represents a subject, each column represents an object, and each entry is the set of access rights for that subject to that object. In general, the access control matrix is sparse: most subjects do not have access rights to most objects. Therefore, different representations have been proposed.").

[11] That path to a global despot follows from the conservative assumption that the power of data fusion is this: every bit of new data increases an exponent in some power equation rather than merely adding to some linear sum. The idea probably first appeared in, Bruce Schneier's *The Myth of the 'Transparent Society'* and David Brin's *Rebuttal*. David Brin, *Defense of a Transparent Society*, WIRED (Mar. 12, 2000), https://www.wired.com/2008/03/brin-rebuttal; Bruce Schneier, *Myth of the 'Transparent Society,'* WIRED (Mar. 6, 2000), www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0306.

[12] Truth in Lending (Regulation Z), 12 C.F.R. § 1026 (2021), https://www.consumerfinance.gov/rules-policy/regulations/1026.

[13] Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html.

[14] *See* Dan Geer, *The Right to be Unobserved*, IEEE S&P (July/Aug. 2015), http://geer.tinho.net/ieee/ieee.sp.geer.1507.pdf.

[15] 31 CFR § 1010.230.

[16] *See* Dan Geer & Paul Vixie, *For Good Measure: Nameless Dread*, 43 ;LOGIN: 53, (2018), http://geer.tinho.net/fgm/fgm.geer.1812.pdf.

[17] What's more, what is the risk interaction of this with an IPv6 world too big to enumerate, not to mention that IPv6 protocols provide address hopping and multi-homing inherently? Will internal firewalls include a key-centric, rather than a name-centric, PKI? Does a MAC address or a UUID-in-ROM distinguish keys in a nameless world and thus imply an identity-based PKI?

Information Society Project
Yale Law School

Published by the Information Society Project at Yale Law School, Baker Hall, 100 Tower Parkway Room 412, New Haven, CT 06520 United States of America.

IMMUTA

The Digital Future Whitepaper Series is made possible thanks to the support of Immuta.

About the Author

Dan Geer is a security researcher with a quantitative bent. He is an electrical engineer (MIT), a statistician (Harvard), and someone who thinks truth is best achieved by adversarial procedures (school of hard knocks). He serves as Senior Fellow at In-Q-Tel. His published work is available at http://geer.tinho.net/pubs.

Digital Future Whitepaper Series

The Digital Future Whitepaper Series, launched in 2020, is a venue for leading global thinkers to question the impact of digital technologies on law and society. The series aims to provide academics, researchers, and practitioners a forum to describe new challenges of data and regulation, to confront core assumptions about law and technology, and to propose new ways to align legal and ethical frameworks to the problems of the digital world.

The Digital Future Whitepaper Series is led by ISP visiting fellow Andrew Burt and co-edited by ISP executive director Nikolas Guggenberger and ISP visiting fellows Artur Pericles Lima Monteiro and Nabiha Syed. Spurthi Jonnalagadda (Yale Law School '22) served as the research assistant for this whitepaper.

Information Society Project

The Information Society Project (ISP) is an intellectual center at Yale Law School, founded in 1997 by Professor Jack Balkin. Over the past twenty years, the ISP has grown from a handful of people gathering to discuss internet governance into an international community working to illuminate the complex relationships between law, technology, and society.

Information Society Project
Yale Law School

127 Wall Street
New Haven, CT 06511

203.432.4992
www.law.yale.edu/isp