PASSWORDS

PHILOLOGY, SECURITY, AUTHENTICATION

BRIAN LENNON

Brian Lennon is associate professor of English and comparative literature at Pennsylvania State University. He is the author of *In Babel's Shadow: Multilingual Literatures, Monolingual States* (University of Minnesota Press, 2010).

The main philosophical tradition of thought about language in the West, Umberto Eco wrote before the turn of the millennium, is a "dream that has run now for almost two thousand years."[1] It is a dream of perfectible representation—not the same as *perfect* representation—which Eco told us had submerged what he called the "pedestrian" account of the flood in Genesis 10:5 in the dramatic and tragic account of Babel in Genesis 11:1, received as a story of human punishment by a vengeful, if wise, God.[2]

Essentially, Eco implied, it was an anti-philological dream: the image of a perfected state in which historical time, and along with time, change—in language, in the history of language, in the order of things managed and maintained by language—might come to cease.

Philology is a secular countertradition to this main philosophical tradition—which is also secular, but also more rationalistic than historicist in its intellectual temperaments, in ways that will leave these two traditions incompatible, even incommensurable. But that is not to say unconfusable, or unconfused. Insofar as we might describe that main tradition—it is a cultural tradition, not merely a "philosophical" one—as a tradition that either presumes or attempts to establish a certain *security,* in the face of time and change and their confusions, including linguistic confusion and an attendant ordinal confusion, we might say also that philology's practices and operations, which are so often practices of *authentication,* enter into conflict with the history, the historicity, and the historiography for which philology stands or stands in, or which it operates.

>>

Three arguments will be left mostly implicit in what follows, as framing a larger project of which this essay is a segment. First, conflict between the philological and the anti-philological imaginations of language is a conflict that structured twentieth-century global cultural history. Second, that conflict has a permanent, non-soluble character. And third, it is an interesting conflict *because* it is non-soluble, all hopes and dreams of the new digital philologists (and anti-philologists) notwithstanding. I draw here on a little book published by Jean Baudrillard in 2000 titled *Mots de passe* (*Passwords*), which served as a recapitulation in keywords of Baudrillard's body of work to that point.[3] The organizing conceit of this text juxtaposes what I will call the philologically figurative connotation of "le mot de passe" / "password" with the technical denotation also invoked by the volume's title.[4] Some of the segments of *Mots de passe* ("La séduction," "La transparence du mal," "Le crime parfait") served as oblique précis of eponymous works or editorial assemblages published under Baudrillard's name in the past; others ("L'objet," "La valeur," "Le virtuel") deployed keywords as such. Together, they provide an index to the matrix of intellectual motives, trajectories, and transitions that took Baudrillard from the early French structuralism and autocritical Marxism of *Le système des objets* (1968, *The System of Objects*) and *Pour une critique de l'économie politique du signe* (1972, *For a Critique of the Political Economy of the Sign*) to the anthropological break with Marxism in *La société de consommation* (1970, *The Consumer Society*) and *Le miroir*

de la production (1973, *The Mirror of Production*) and the "posthistorical" studies of simulation, hyperreality, and terror that brought Baudrillard North American fame in sometimes awkward translation.

The technical denotation of "le mot de passe" is its quotidian sense, raised to a difficult public awareness, in and since 2012, by a series of both massive and well-publicized intrusions aimed at Web 2.0 and social media services mostly based in the United States but operating on networks imagined as worlded or worlding space.[5] It was this series of attacks, accompanied by increasingly severe admonition of "lusers" by those in the know, that finally introduced a counter-discourse at odds with the wave of enthusiasm for consumer utility or cloud computing that a new generation of IT pundits and consultants rode to power in the late 2000s, as the survivors of the dotcom crash reorganized their data service operations.[6] Named the "Year of Security," 2012 has taught us a lesson that, to be sure, was always there to be learned, which is that since the very beginning of the long march of component miniaturization that brought us the personal computer in the late 1970s—but is virtually coterminous with digital computing itself—a password provides effective security only to the extent that it is *not* a word; or, to put it more (or less) concretely, when it can no longer be found in a dictionary, that chain of signifiers stable or sliding as the case may be. As an elementary form of assault on password security, automated dictionary attacks, which submit all entries in a dictionary to an authentication mechanism, ensure that the strongest password is a pseudo-random assemblage of characters, impossible for a human being to guess and so impossible for a human being to remember, requiring storage in a local electronic password safe or, ideally, physically secured—for example, recorded on a piece of paper placed in a safe secured by a combination lock and bolted to the floor, as information security becomes physical security becomes information security once again.

We might say that the technical function of the password is to thwart time in the name of security: to verify, by means of an invariant linguistic signature, that for the purpose of access to resources, I am the same user I was yesterday.

We might say that the technical function of the password is to thwart time in the name of security: to verify, by means of an invariant linguistic signature, that for the purpose of access to resources, I am the same user I was yesterday. The password permits me, the user possessing it, to pass, and serves as a pass or key, a promise that nothing has changed.

Contrariwise, we might say that the philological connotation of "password" marks a commitment to the recognition, even the embrace, of time, of time's passing rather than my passing—or else precisely my passing, in another sense again, that of time's passing "over" and through me: of an irreducible insecurity. A word, Baudrillard insists in *Passwords,* is temporal, a metaphorization that bears or passes ideas, exerting form on

thought in passing away. That words "have a life of their own and, hence, are mortal is evident to anyone who does not claim to possess a definitive form of thought, with ambitions to edify."[7]

>>

We might say that Baudrillard thus points to a historic conflict between two intellectual temperaments: to a schism with both real and imagined power, through which secular historical or historicizing humanism, orienting itself in and by time, opposes an anti-philological technocratic thinking that seeks to mitigate time.

To be sure, a structure can be built over that great divide, masking its incommensurability. The relation of a strong password, taken as a signifier, to its signified is technically arbitrary. Imposed for the occasion, it is no less purely relational than any signature, since its function is not to *be* but to differ. A strong password is of course also conventionally or historically arbitrary, in the sense that it is chosen at a particular place and time, is subject to degradation in time, and requires renewal if it is to continue to perform its function: that is, to differ. Yet such change is itself technical in character, a reconstruction of structural difference against temporal deferral, intended to preserve the security of the immutable that authentication provides, defends, and presumes or requires all at once. One changes one's password to preempt its degradation in time, as storage follows use, exposure threatens storage, brute force computational attack follows exposure, and identity masquerade follows a successful attack. Even where it is a strong password and thus nothing like a word at all, the password suffers the passing that time imposes on language, and which literary language perhaps merely accents with constructed polysemy. As InfoSec professionals have always known, but ordinary "lusers" are only now coming to understand, the strongest password serves as a one-way function, easy to formulate but difficult to invert, at least within the limit of the computing power available at a given moment.

Baudrillard's work was a sustained refusal of the unilateral concept of communication derived from information theory, which inscribed the telematic trigram *encoder/transmitter → message → decoder/receiver* onto the "reversible" bilateral ambivalence of human symbolic exchange:

> Symbolic exchange is the strategic site where all the modalities of value flow together towards what I would term a blind zone, in which everything is called into question again. The symbolic here does not have the usual sense of "imaginary," nor the sense given to it by Lacan. It is symbolic exchange as anthropology understands it. Whereas value always has a unidirectional sense, whereas it passes from one point to another according to a system of equivalence, in symbolic exchange the terms are reversible.[8]

In Baudrillard's work the "cybernetic semioticization" of the media—its atemporal, indeed time-repellent, hyper-circulation of hyper-legible signs—appeared as a simulation of such reversibility in feedback, the autoimmune integration of reciprocity and

exteriority designed to forestall any compromise (human or otherwise) of abstract systemic integrity.[9] Baudrillard never really succumbed to the French fascination by cybernetics recently explored at some length by Lydia Liu, John Johnston, and Bernard Dionysius Geoghegan, among others;[10] indeed, for all the intellectually violent dynamism of his both saturnine and mercurial oeuvre, Baudrillard seems quite consistently to have opposed the stakes of that fascination, counterposing to it an antipositivism derived from elements of the historical legacy of ethnology, including philology. In many ways the ethically strongest element of Baudrillard's work is this resistance to the restructuring of intellectual life as what Geoghegan calls "crypto-intelligence,"[11] in the conversion of human discourse to the antagonistic exchange and interception of encrypted mail. As a one-way function, easy to formulate but difficult to invert, a properly strong password is a guarantor of unilateral communication, ensuring that an encrypted message cannot be intercepted, altered, or redirected. It is also an instance of such guaranteed communication itself.

>>

J. Frederik M. Arends opens his brief history of the Western concept of security by admitting that "to study the history of concepts seems the innocent pastime of philological hobbyists."[12] The retraction that follows ("at least in the case of the concept of 'security' that judgment might prove to be a misunderstanding"[13]) might be said to serve as a placing of philology under erasure, in so far as the "insecurity" of words that marks their historicity is identified as a border zone needing as much critical interrogation as observation—or, to put it in terms of the strife of faculties, as that which "security studies" must disavow, at least temporarily, in order to constitute itself as an academic discipline.

Distinguishing two phases in the etymological, philosophical, and ideological history of security, Arends suggests that the polysemy of classical Latin *securitas,* denoting the "freedom from care" of the Pax Romana but also used by the Romans with a second, negative connotation (carelessness, negligence, complacency), was attenuated by the narrower early Christian usage associated with faith and contrasted with *dubitatio.* Subsequently, Arends suggests, the narrower early Christian usage would be displaced in theology, at least, by the medieval Latin *certitudo.* But the modern concept of "security" emerged with Hobbes, mediated by Hobbes's translation of Thucydides's *History of the Peloponnesian War.* Retaining nothing of the ambivalence of Roman *securitas,* Arends argues, Thucydides, the chronicler of the Athenian empire and its civil war, employs the word and concept *asphaleia* (immovability, derived from the verb *sphallō,* associated with wrestling and used metaphorically to describe the stability of an institution) as a substantive for the Athenian state threatened by civil war.[14] Hobbes's induction from a "Thucydidean anthropology" to a Lucretian "mathematical foundation independent of party strife," Arends concludes, represents an attempt to mediate modern secularization by stabilizing the meaning of a concept, expressed metaphorically in the consensus of subjection to the state as a guarantor of punishment for violations of law.[15]

A similar dynamic has been identified in formulations of US foreign policy, for example, in the aftermath of the Second World War, as "security" was elevated over the companion keywords "peace" and "safety" that had accompanied it in Woodrow Wilson's Fourteen Points declaration and in the 1919 Covenant of the League of Nations, and throughout the presidency of Franklin Delano Roosevelt, while the internally constituted rights of both citizens and noncitizens described by the 1935 Social Security Act, the 1941 Atlantic Charter, and the 1948 Universal Declaration of Human Rights were reclassified with the modifier term "social."[16] In both cases, Arends suggests, we might speak of the institutional hypostatization of security as a kind of "idée directrice," effectively a (re-)sacralization of what Andrea Schrimm-Heins calls the "secularization of *certitudo*" achieved in philosophy's modern emancipation from theology:[17] what we might call its Leviathanization, binding a historically polysemous word and concept tightly to a circumscriptive association with social order.[18]

>>

Though information security is reflexively linked to the technological history of modern telecommunications, it might just as sensibly be understood as a core administrative concern of the states of the ancient world, and thus as coterminous with the historical origin of writing itself. It is also just as plausible that something historically unprecedented inheres in the acceleration and integration made possible by digital computing, in relation to security as to anything else. Indeed, one assessment has emphasized the "unprecedented civilian deployment of security tools and technologies" in the information societies of the historical present.[19]

Electronic information security depends on the authentication of identities and data, a procedure marked by a single antinomian principle and set of concepts associated with it. A thinking InfoSec professional operates on the assumption that every new security enhancement produces a new security risk, by presenting attackers with new means and opportunities for technically (and non-technically) compromising any given system or class of systems. "If a person can trust keeping belongings in a locked compartment," as Pieter Wisse puts it, "then it is the key that should be of concern."[20] The physical security perimeters of massive early mainframe computers, with material (often military) installations removable, in material space, to a material distance from any given attacker, had been obviated by the 1970s by two mundane elements of personal computing: network connectivity and the portability made possible by component miniaturization.

But electronic information security also rests on a concept of availability inflected by the relative immateriality of data and its elementary reproducibility, which under everyday conditions leaves data remarkably persistent. Under such conditions, there is nothing to compromise only when no information has been stored or transmitted at all, and perfect security can be ensured only by not recording or transmitting in the first place. As many a Facebook user discovers anew, every few months, the confidentiality of data in storage or transmission will always be undermined by its availability to someone, even if that someone is a single user.

Electronic authentication regulates access to data that is already available in this sense. An authentication mechanism manages the identities of users, granting access to resources with different levels of privilege codified for classes of identities and granting different mixtures of rights to resource ownership and access. While on structurally complex systems, there is no meaningful limit to the hierarchical differentiation of this matrix of privilege (even the most basic versions of the Unix-type multiuser permissions schemes still in use permit many permutations), the clear differentiation and assignation of interactive roles are unavoidable, and as a first step always separate the administrators of a given system from the users on whose behalf they manage services. Usually, administrators manage services for the system's proprietor, in liaison with a telecommunications carrier that links the system to others outside its domain. Any relationship to a given system is marked by its interiority or exteriority, in this sense, and relation—in some ways, the very possibility of relation—with an outsider is considered an attack.[21]

So-called TEMPEST standards for electromagnetic shielding, developed to defend equipment from the close-range radiation emission attacks directed against electromechanical cipher machines, mark the first recognition of the intrinsic hazard of availability in computing systems. Networking over telephone lines, introduced with the US Air Force SAGE (Semi-Automatic Ground Environment) air defense system in the late 1950s, brought with it the threat of "man in the middle" interception, and the time-sharing systems of the early 1960s are generally understood to have forced what Jeffrey R. Yost calls a sea change in computer security.[22] Though the multiplexing of dumb terminals attached to mainframes allocating processing cycles, memory, and data storage to multiple simultaneous users was far more efficient and convenient (for some) than the manual and batch processing systems preceding them, their multiple differentiated levels of access proved incompatible with military document classification and clearance protocols.[23] Accompanied by rapid growth in software complexity, it was the widespread adoption of time-sharing systems that more than anything else brought the computer security problem to historical maturity, with the early 1970s work of David Elliott Bell and Leonard J. LaPadula on a multiuser, multilevel security model for the US Air Force marking the emergence of computer security as a distinct research area.[24]

From that point on, those employed to protect information security and those attempting to compromise it would be locked in the dialectic marked by the iconography of white, black, and gray hats today.[25] The later 1970s would bring the first preassembled commercial personal computers, removable storage media, Bulletin Board Systems (BBS) run on public telephone networks, software viruses, and the emergence of a hacker group youth subculture. By the 1980s, computer security was a topic of popular culture (such as the 1983 film *War Games*) and public awareness, especially following the Morris worm of 1988 and the formation of the first US Computer Emergency Response Team (CERT). The 1990s have been called the "contagion period" of early public Internet use,[26] with the Netscape browser incorporating RSA and SSL public key algorithms to provide for encrypted commercial transactions, on the one hand, and the emergence of new forms of both advertising and criminality (spam email, spyware, denial of service

and distributed denial of service [DDoS] attacks on Web sites, launched by virus-infected "botnets" of Internet-connected home and business PCs) on the other, in turn spurring the development of commercial firewall software, virtual private network (VPN) services, and authentication products like RSA SecurID.[27]

>>

If computer user authentication has employed software-based encryption almost from the very start, that is no reason to abstract it from the material and intellectual history of modern authentication techniques beginning with currency watermarking and security printing, developing further with modern state militarization, imperial conquest and colonization, internal policing, border control, and secular education, and culminating in the automated biometric techniques of today.[28] Unlike serial manual or batch processing conventions for computer programming, in which sets of instructions were processed serially (initially, in a strict division of labor, by dedicated computer operators who configured instructions, triggered processing, and returned the results to a user), time-sharing systems were interactive, permitting multiple authorized users both direct and limited access to apportioned computing resources. The Compatible Time-Sharing System designed at MIT in 1961 assigned each user a username linked to storage space for personal files accessed using a stored plaintext passcode, as did the Unics (Unix) systems developed at Bell Labs later in the 1960s. Users of such systems, often students, promptly began probing their multiplexing architecture—and the hacker was born.[29] From that point forward, as Richard E. Smith put it, computer authentication systems evolved under attack, in a dynamic illustration of what we might have to call the law of the insecurity of security, which ensures that the possibility of masquerade can never be eliminated entirely, given that no new security mechanism could ever solve a security problem permanently, while every advance in security techniques simultaneously offers new exploits to potential attackers.[30] When the Titan system at Cambridge University, followed by the Unix systems, added cryptographic hashing to protect stored password files from theft by users with unauthorized access,

Computer authentication systems evolved under attack, in a dynamic illustration of what we might have to call the law of the insecurity of security, which ensures that the possibility of masquerade can never be eliminated entirely, given that no new security mechanism could ever solve a security problem permanently, while every advance in security techniques simultaneously offers new exploits to potential attackers.

attackers shifted their efforts to the interception of passwords using key sniffing and logging software that records keystrokes, and a new round of competition ensued.

The endurance of this social and technical dialectic suggests on the one hand that perfect information security is effectively a metaphysical concept, transcending any worldly implementation—and on the other that the practical usability of any system simply and irreducibly requires a measure of trust, that form of security that can never be consummated beyond all limit of possible loss or violation.

>>

As Smith describes it, an authentication mechanism performs identification before granting access, relying on a "base secret" possessed by the user and serving as a distinguishing characteristic.[31] In practice, many such characteristics are straightforwardly cultural in character, so that it makes sense to speak of some forms of authentication themselves as cultural rituals. Cultural authentication involves base secrets that are not arbitrary, often not frequently or easily changed, and subject to exposure (one's mother's so-called maiden name, for example—which in a society in which many married women do not take their partner's name, or who divorce at a rate higher than a few percent, is a very weak secret indeed). What we call shibboleths, or recognizable marks of communal membership ascertained through various kinds of tests, are perhaps the best example—from the shibboleth incident narrated in the Old Testament book of Judges, in which the base secret is the difference between local dialects,[32] to the twenty-first-century academic resource-sharing system that takes its name from the biblical story.[33]

In contrast with modes of cultural authentication, pseudo-random authentication—relying on a secret such as a pseudo-random numeric or mixed alphabetic and numeric code—is more secure insofar as it is not a secret shared by one's cultural or social group, but something assigned to an individual, personally possessed often in a physical sense, and requiring interception or capture in order to compromise (for example, a credit card number). But the arbitrary character of pseudo-random passcodes makes them difficult to remember, and they need to be synchronized in advance in order to be useful. Arguably, the folkloric scenario involving a password spoken to the guard at a medieval city gate combines elements of cultural and random authentication, with the answer to the guard's challenge being something not easily guessed by unauthorized strangers, yet not granting unconditional access, either, instead merely serving to supplement visual identification.[34]

The folktale of Ali Baba and the forty thieves—in which the password by itself suffices, through the intermediation of some mechanism that opens a door, to grant access to the cave—is in fact closer to the single-factor "unattended" authentication on which much consumer computing still relies today.[35] Technically imagined, the thieves' cave is protected by an "unattended, password-controlled lock . . . an unexplained and probably magical device that mechanically responded to the spoken words" *Sésame, ouvre-toi*.[36] As a mechanical authentication system, what guards the cave resembles a combination lock

or a computer password system in that anyone who possesses the secret, regardless of intent or disposition in relation to what it secures, can masquerade as the authorized user: the system actually authenticates only the password itself, not the user providing it.[37]

>>

As the oldest and still most convenient form of electronic authentication, password authentication mechanisms identify each user with a username and test for the user's distinguishing characteristic: possession of the secret password.[38] Most systems accomplish this by comparing user input of the password with a stored system record synchronized with the user at the time that an authorized account is first established, and the earliest technical attacks on password systems were directed at that stored record itself. This is precisely why what we call "words"—the lexemes of a particular human language and writing system, marked by statistical unit frequency patterns of various kinds (letters, digraphs, trigraphs) that computers can analyze quickly and efficiently—make the weakest passwords.[39] Taking advantage of human difficulty in memorizing random information, and the resulting tendency for users to select actual (and often personally meaningful) words as passwords, so-called dictionary attacks simply submit all the entries in a compiled dictionary to an authentication mechanism. Encryption or hashing of passwords adds little real security to any password contained in a dictionary if an attacker is able to generate cryptographic hashes of dictionary words themselves (in other words, to hash the entire dictionary) and then compare them with hash signatures in a password file.[40]

As a mechanical authentication system, what guards the cave resembles a combination lock or a computer password system in that anyone who possesses the secret, regardless of intent or disposition in relation to what it secures, can masquerade as the authorized user: the system actually authenticates only the password itself, not the user providing it.

Rooted in widespread consumer and enterprise ignorance when it comes to how authentication mechanisms operate and how they can be compromised, poor judgment in selecting passwords is now considered a security threat of the highest order, with the intractability of the problem spurring many a recent commentator to declare password authentication fundamentally broken.[41] Recommendations initially formulated in the late 1980s, according to which passwords should include letters in mixed lower- and uppercase, digits, and punctuation, are no more consistently implemented today than they were thirty years ago; behind such "classical" password selection rules, Smith notes, is an imagination of perfect security in which "the password must be impossible

to remember and never written down." In what Smith calls the "rather bizarre duality of security tools and attack tools," the defensive tools that screen user passwords to evaluate their strength are just as easy to use as password cracking utilities.[42] Proactive password evaluation "occasionally produces an 'arms race' between the user community and the people responsible for password enforcement. The users keep finding shortcuts and mnemonics while password software designers keep tightening up the constraints on acceptable passwords."[43] At a certain point, requirements for practical password security will impair the practical usability of a system taken as a whole: "Without extensive training, people would not know how to construct legal passwords and would have trouble understanding why their personal choices were rejected. Under such circumstances, a user community is more likely to accept machine-generated passwords, since the draconian rules make a mockery of the concept of personal choice."[44]

Unable to memorize automatically generated, pseudo-random passwords, and prompted frequently to change them, users resort to measures that compromise the security of any password system entirely, such as keeping a written copy of the password nearby (for example, under their mouse pads).[45] The future of authentication thus appears, for now at least, to lie in multiple-factor authentication making use of biometric techniques and physical tokens such as electronic smart cards and keys—a development that may bring the linguistic, even literary history of account-based electronic access control to an end.

>>

In the technical literature on password authentication, the linguistic and literary history of the password begins with the so-called shibboleth incident. Judges 12 contains an account of a battle between the Gileadites and Ephraimites, at one point during which the retreating Ephraimites, attempting to cross a river in Gileadite territory, were challenged by the Gileadites to identify themselves by pronouncing the word שבלת (*shibboleth*). With the suggestion that the Ephraimites' pronunciation, סבלת (*sibboleth*), substituting ס (*samekh*) for ש (*shin*), gave them away, we are told that the Gileadites slaughtered forty-two thousand of them on the spot:

> And capture did Gilead the fords of the Jordan against Ephraim.
> And when the fugitives of Ephraim would say,
> "Let me cross,"
> say to him would the men of Gilead,
> "An Ephraimite are you?"
> And he would say, "No,"
> And they would say to him,
> "Say, pray, 'shibboleth,'"
> and he would say "sibboleth,"
> And he could not accomplish to say it thus,

and they would seize him and slaughter him at the fords of the Jordan.
And fall at that time from Ephraim did forty-two thousand.[46]

This first "password" in Western literature appears in nineteen places in the Hebrew Bible in all and in sixteen places in the Old Testament.[47] *Shibboleth* is understood to have had two different denotations in Biblical Hebrew: the first, ear of grain or corn ("olive branch" has also been proposed), is the most common, while the second, flood or torrent of water in a stream, appears unambiguously in only two of the sixteen appearances of *shibboleth* in the Old Testament.[48] While this second, less common meaning is more plainly related to the context of the shibboleth story, it is not unambiguously clear which of the two meanings the word is meant to carry in this particular context, though in many similar legends, the meaning of the "password" does usually relate in some way to the context.[49]

The *Oxford English Dictionary* offers three meanings for "shibboleth" dating to the seventeenth century: one, "a word used as a test for detecting foreigners," linked to the testing function described in the biblical story; another, "a peculiarity of pronunciation or accent indicative of a person's origin," denoting an identifying distinction in itself; and a third closer to the contemporary journalistic sense in which, as Jennifer Michael suggests, the phrase "family values" might be described as a shibboleth: "a catchword or formula adopted by a party or sect, by which their adherents or followers may be discerned, or those not their followers may be excluded."[50]

In much academic scholarship, the word is used in ways that track rather closely these earlier meanings.[51] Recent work in sociolinguistics and the sociology of language has treated shibboleths as elements of "everyday verbal behavior,"[52] including phonological elements of computer-mediated written communication,[53] or returned to the word's scriptural origins—arguing, for example, that Australian government language proficiency tests should be understood as "weapons in the tradition of the Shibboleth test," less performance tests than means of detection and identification in border control.[54] In folklore studies, "shibboleth" is given the wider nineteenth-century sense provided by the *OED,* which also encompasses the extralinguistic ("a custom, habit, mode of dress, or the like, which distinguishes a particular class or set of persons"). Michael, for example, distinguishes between "exclusion shibboleths" designed to prevent access by outsiders and "inclusion shibboleths" including indoctrination rituals that make joining a community possible with effort, suggesting that we consider forms of dress as "somatic" shibboleths.[55]

Pack Carnes, meanwhile, calls a large body of similar legends "neck legends," from apocryphal stories about testing for the aristocratic pronunciation of the word "moi" during the French Revolution. Such stories, Carnes notes, are numerous, often involve warfare, and tend not to depict reliable tests or to involve great difficulty for the speaker being tested; they rather represent difficulties that a non-native speaker is assumed by caricature to have with a particular, putatively native language in a particular context, and almost always depict a failure to pass the test.[56] More or less frequently cited

examples include English use of the place-name "Chichester Church" to identify Danes during the St. Brice's Day massacre of 1002;[57] Sicilian use of the phrase "ceci e ciceri" to identify the French during the rebellion of 1282;[58] use of a phrase in Frisian to identify the Dutch during the Battle of Warns in 1345;[59] use of the phrase "bread and cheese" to identify the Flemish during Wat Tyler's peasants' revolt in 1381;[60] use of regional variations in the pronunciation of the word "cow" in 1850s Bleeding Kansas;[61] the phrase "setze jutges mengen fetge d'un jutjat" (sixteen judges from a court eat the liver of a hanged man) used to identify Castilian immigrants in Catalonia;[62] and an abundance of anecdotes from the Second World War and subsequent conflicts, including the pronunciation of Levantine Arabic *bandora* (tomato), used by the Phalangists to identify Palestinians in the 1970s and1980s, and of Sinhala *baldiya* (bucket), used by Sinhalese to identify Tamils during the first year of the Sri Lankan civil war.[63]

>>

It seems most sensible to read the shibboleth incident with Marc Brettler, as a political allegory in which the signifier "Ephraim" serves as a "general epithet" for northern Canaan, rather than denominating the tribe of Ephraim specifically.[64] With the exception of David Marcus, who insists that we take the shibboleth incident as satire,[65] much of the philological scholarship on Judges 12:6 itself is narrowly technical in character, seeking to secure and authenticate the derivation and etymological history of שבלת *shibboleth*. Where that debate is drawn toward the *interpretation* of the story told in Judges, it tends to divide on the question of whether *shibboleth* serves or does not serve as a "password" in something close to the technical sense: that is, the question of whether the denotation of *shibboleth,* whether it be "ear of grain, corn" or "flood, torrent of water in a stream," has any meaning in and for the story at all—or whether on the other hand what is depicted in the shibboleth story is purely cultural authentication, a "test-word episode" that turns on its pronunciation in different Hebrew dialects.[66]

George Foot Moore, for example, argued that "any other word beginning with *sh* would have served as well," and that contemporary readers have construed *shibboleth* as a "password" only because the Greek of the Septuagint "had no way of reproducing the distinction of sounds represented."[67] From this perspective, the meaning of *shibboleth* is irrelevant to the story, because the story depicts a test of pronunciation of the initial sibilant written either as ש or as ס in the Gileadite and Ephraimite dialects: the initial sibilant of שבלת *shibboleth* is, in other words, "the point of the test, and . . . inability to pronounce it like the Gileadites was the Ephraimite problem."[68] Judean scribes, it is argued, represented this phonetic difference by deliberately choosing ס to represent the non-representable phonetic difference of the Ephraimite pronunciation of a Gileadite spirant.[69]

But by the same token, *shibboleth* can be imagined as a password in a figurative sense, one more expansively than restrictively or technically philological. Just to the extent that its denotation is insignificant—to the extent that it functions merely to test for a phonological differential characteristic that the Judean scribes were unable to represent

in writing—the shibboleth is a mark of passing or a trace of that difference, the "insignificant arbitrary mark" of a "secret without secrecy": its resistance to translation, including translations of the text of Judges 12, is not the resistance of secret meaning, but of the "cut of the non-signifying difference."[70] Marcus takes this approach in another direction, and to something of an extreme, rejecting the idea of dialectal difference and thus all of the more traditional restrictively philological debate along with it. Marcus concludes that the shibboleth story is a Judean satire written to ridicule the Ephraimites, the dominant tribe during the period of the Judges, "as ignorant nincompoops who cannot even repeat a test-word spoken by the Gileadites' guards."[71]

>>

In addition to the shibboleth story in Judges 12, the technical literature on password authentication has embraced a second literary antecedent: the tale of Ali Baba and the forty thieves.[72] Here, too, we are dealing with another foundational artifact of Western literary history, insofar as a ninth-century fragment of *Alf Layla* or *Thousand Nights,* the collection of tales to which Antoine Galland (1646–1715) would add the tale "Ali Baba et les quarante voleurs" in the eighteenth century, was the oldest known surviving artifact of an Arabic paper book. Imagined by Tzvetan Todorov as an "extreme example" of the literary "a-psychologism" of the *Nights* as a whole, populated by "narrative-men" who "illustrate" nothing but are subservient to the action,[73] the tale describes a magical cave whose opening is unsealed by the pronouncement "Sésame, ouvre-toi" ("Open, Sesame!").

Here, too, much traditionally philological scholarship has sought to authenticate by securing a key "password": in this case, "sésame." Supposing that Galland worked from Hanna Diab's written Arabic, and that the word at issue was thus the Arabic *símsim*,[74] F. E. Peiser suggested it was a duplication of שם *shem* "name," the Hebrew word for God that appears in Leviticus 24:11, or else a cabbalistic invocation, the Talmudic שם שמים *shem-shemayim* "name of heaven."[75] This, Paul Haupt subsequently declared, was fanciful: *símsim* need not mean "sesame" in the context of the description of the cave, Kasim's attempting the names of other grains notwithstanding.[76] *Símsim* may instead, Haupt suggested, represent a modern Arabic pronunciation of an older word meaning "stopper, shutter, barrier."[77] But Haupt also noted parallel locutions in similar tales in Chinese, modern Greek, and German (the Grimms recorded a tale entitled "Simeliberg," possibly referring to a mountain in Grabfeld [Bavaria] and containing the locutions "Open Simsi!" and "Open Simeli"), suggesting that something more (or less) was at stake than linguistic genealogies.

>>

Incorporated thus into the technical literature on authentication and on information security more generally, as precedents for technical operations that the philological scholarship devoted to them both mimics and complicates, these two literary artifacts

occupy a site where technical history crosses literary history and the history of philology, as the practice of the verification of written sources as historical and human, rather than divine. Following the work and the example of Edward W. Said, late twentieth- and early twenty-first-century returns to philology[78] have sought to salvage the secular historical humanism of modern philology by extricating it at least partly from its imbrication with the scholarly Orientalism of the European empires and its transmogrified afterlife in the applied social science of a new postwar US security state.[79] It is understandable that such revisionist concepts of philology have often resisted its associations with scientism, positivism, and the charisma of authority, in a way that might be taken as conflating, for better or for worse, the security of truth with the security of the state.[80] And yet, it is precisely in retaining a reasonable valuation of reason itself, of recent inquiry, and of science if not of scientism, that such work has often also been able to insist, suggestively, that such conflation is not merely an act of the will or imagination, either. Seth Lerer's glib yet piquant collation of the philological impulse with a charismatic-authoritarian egoistic need for "security" has put some of his interlocutors on the defensive for a good reason, even if their counter-critiques are also reasonable.[81] To make headway here, we need to move beyond disputes rooted in intellectual dispositions and their conflicts, to the material institutional context in which such dispositions are formed. Ronald A. T. Judy has written of secular education as the guarantor of a civil society in the United States, with both liberal arts colleges and the research universities that followed them serving to regulate discourse through the classical humanist curriculum (in the first case) and the professionalization of the human sciences (in the second).[82] Somewhat more explicit is the work of Henry Veggian, tracing a line of transmission from the Franco-Prussian War to the French *Bureau du Chiffre* and the literary-critical origins of US military cryptology—that is, from nineteenth-century German philology to literary criticism as we know it today, by way of modern military intelligence.[83] Far from being outlandish in character, the relationship between military intelligence and literary scholarship, Veggian has observed, is perfectly mundane, marking philological practices that would escape philology in a mathematization sponsored by the security state, as philology was dispersed into other sciences.[84] The latest chapter in this story, which has drawn a corps of new "digital" humanists to symbologically serve the surveillance state produced by the security crisis of 2001, has yet to be told.

Notes

1 Eco, *The Search for the Perfect Language,* 5.

2 Ibid., 9–10.

3 *Mots de passe* was produced in conjunction with a documentary film, *Mots de passe: Jean Baudrillard,* by Pierre Bourgeois and Leslie Grunberg, portions of which can be viewed on the website of the European Graduate School: http://www.egs.edu/faculty/jean-baudrillard/videos/mots-de-passe-passwords/.

4 "Le mot de passe" is the everyday French equivalent for the technical denotation of the English "password," though of course it can be used figuratively in French just as it can be in English.

5 See Ken Hess, "2012: The Year of Security"—little more than a squib, but one that anticipated a truly dramatic year. Since then, malware-based espionage and data theft sponsored by both nation-states and organized crime have escalated so dramatically that any catalog of spectacular exploits would be stale information within months, if not weeks.

6 "Luser" is a portmanteau word combining "user" and "loser," used by IT service providers to describe those whom they serve.

7 Baudrillard, *Passwords,* xiii.

8 Ibid., 15.

9 See William Merrin, *Baudrillard and the Media,* 16. Of the intellectual-historical development through which "Western modernity has increasingly seen the world as language," Richard Terdiman observes, "such systems *take no time*. Through their rule-boundedness, logics repel temporality, and structuralist models aggressively repudiate it. . . . Paradigms based on language have a low aptitude for modeling time in its productivity" ("Taking Time," 136–37).

10 See Liu, *The Freudian Robot;* Johnston, *The Allure of Machinic Life;* Geoghegan, "Agents of History"; Geoghegan, "From Information Theory to French Theory."

11 Geoghegan, "Agents of History," 405.

12 Arends, "From Homer to Hobbes and Beyond," 263.

13 Ibid.

14 Ibid., 265–66.

15 Ibid., 272.

16 Arends draws here on Czempiel, *Das amerikanische Sicherheitssystem 1945–1949,* 60, and Kaufmann, *Sicherheit als soziologisches und sozialpolitisches Problem,* 13, 71n21, 72n22 (Arends, "From Homer to Hobbes and Beyond," 275).

17 Arends, "From Homer to Hobbes and Beyond," 277.

18 See also Schrimm-Heins, "Gewißheit und Sicherheit," as cited in Arends, "From Homer to Hobbes and Beyond," 277.

19 de Leeuw, introduction to *The History of Information Security*, edited by de Leeuw and Berstra, 24.

20 Wisse, "Semiotics of Identity Management," 191.

21 Smith, *Authentication: From Passwords to Public Keys,* 73–77.

22 Yost, "A History of Computer Security Standards," 602.

23 Ibid. See also Michael Warner, "Cybersecurity: A Pre-history"—a useful "pre-history" of the "cybersecurity problem" that might seem otherwise to have emerged so abruptly in 2012.

24 Yost, "A History of Computer Security Standards," 642. See Bell and LaPadula, *Secure Computer Systems: Mathematical Foundations,* and *Secure Computer System: Unified Exposition and Multics Interpretation.*

25 A hacker who tests systems for their proprietors (almost always as a contracted professional) dons an imagined "white hat," while a "black hat" hacker conducts criminal exploits. One of the many ways to define a "gray hat" hacker is as someone who employs the methods of the latter for the purposes of the former.

26 van Biene-Hershey, "IT Security and IT Auditing between 1960 and 2000," 675–76.

27 See Brenner, "History of Computer Crime," 709.

28 On the history and current deployment of biometric techniques, see Higgs, "From Frankpledge to Chip and PIN"; Schell, "History of Document Security"; Wayman, "The Scientific Development of Biometrics over the Last 40 Years"; Wisse, "Semiotics of Identity Management."

29 Smith, *Authentication: From Passwords to Public Keys,* 11.

30 Schell, "History of Document Security," 204. A lock, for example, merely shifts the security "problem" to control of access to the key (Smith, *Authentication*, 5). Schell notes that every advance in techniques of reproduction for currency printing has always also marked an advance in techniques of currency forgery ("History of Document Security," 204).

31 Smith, *Authentication,* 43.

32 This is Smith's way of putting it (perhaps not one that many scholars of Judges would accept; see my further discussion below). See ibid., 45.

33 The Shibboleth system is designed to facilitate the sharing of resources (for example, across university library systems) while preserving a user's individual privacy. A user authenticates with her or his home institution (this being the "cultural" dimension of membership in a particular community), which then passes only as much information about the user as strictly necessary to the "federalized" resource provider (for example, an electronic publisher). (A "Where Are You From?" service directs visitors to Shibboleth servers back to authentication mechanisms at their own institutions.) See Needleman, "The Shibboleth Authentication/Authorization System."

34 Smith, *Authentication,* 39.

35 Ibid., 1.

36 Ibid., 2. (Smith uses the English "Open, Sesame!")

37 Ibid.

38 Ibid.

39 Ibid., 88–89.

40 The defensive tactic called "salting" responds to this vulnerability. Passwords are hashed using a pseudo-random variable or "salt" added to the original data, to ensure that successive hashes of the same password will be non-identical. See ibid., 57.

41 See, for example, Honan, "It's Time to Abandon Passwords"; Newman, "The Username/Password System Is Broken"; Stross, "Goodbye, Passwords. You Aren't a Good Defense."

42 Smith, *Authentication,* 95.

43 Ibid., 97.

44 Ibid.

45 Ibid., 162.

46 Judges 12:4–6; Susan Niditch's literal, lineated translation. See Niditch, *Judges: A Commentary,* 136–38, 252.

47 Marcus, "The Word *Šibboleth* Again"; Hendel, "Sibilants and *Šibbōlet,*" 69.

48 Marcus, "The Word *Šibboleth* Again," 39.

49 Nagai, "Dream Shibboleth," 428. Nagai gives "shibboleth" more literary and philosophical color than one finds in etymological debates among A. F. L. Beeston, Alice Faber, Ronald S. Hendel, Gary A. Rendsburg, Pierre Swiggers, and Robert Woodhouse. But on this point, see also Hendel, "Sibilants and *Šibbōlet,*" 69; Rendsburg, "The Ammonite Phoneme /T/," 75; Rendsburg, "More on Hebrew *Šibbōlet,*" 256; and Swiggers, "The Word *Šibbōlet* in Jud. xii.6," 205.

50 Michael, "(Ad)Dressing Shibboleths," 148.

51 Ibid.

52 Kniffka, "Shibboleths," 159.

53 Ifukor, "Spelling and Simulated Shibboleths in Nigerian Computer-Mediated Communication," 37.

54 McNamara, "21st Century Shibboleth," 351–52.

55 Michael, "(Ad)Dressing Shibboleths," 151–53.

56 Carnes, "'Then Say *Shibboleth*,'" 16–17.

57 Gaster, *Myth, Legend, and Custom in the Old Testament,* 433.

58 Moore, *A Critical and Exegetical Commentary on Judges,* 308.

59 Cramer, "Shibboleth," 36.

60 Gaster, *Myth, Legend, and Custom in the Old Testament,* 433.

61 Etcheson, *Bleeding Kansas*, 118–19.

62 Noyes, "Group," 465.

63 McNamara, "21st Century Shibboleth," 353.

64 Brettler, "The Book of Judges," 408.

65 Marcus, "Ridiculing the Ephraimites," 100.

66 Ibid., 95. The Ephraimites, it is noted, were challenged to pronounce a word, not asked to produce the name of something they were shown or referred to. See Speiser, "The Shibboleth Incident (Judges 12:6)," 10; Marcus, "Ridiculing the Ephraimites," 100.

67 Moore, *A Critical and Exegetical Commentary on Judges,* 308–9. Niditch notes that Judges 12:6 is one of the only passages in the Hebrew Bible, apart from the Babel story, that distinguishes between accents or dialects (*Judges: A Commentary,* 138).

68 Hendel, "Sibilants and *Šibbōlet,*" 71.

69 Swiggers, "The Word *Šibbōlet* in Jud. xii.6," 207.

70 Derrida, "Shibboleth: For Paul Celan," 29–32. Derrida's work on this topic appears to have had little or no influence on the other scholarship I cite here, which in some ways is understandable. One exception is Mieke Bal, who acknowledged the inversion in describing the shibboleth as a "reversed password," a non-secret "silent word that has no meaning, that is pure force" (*Death and Dissymmetry*, 164). By contrast, Susan Stuart describes what she calls "pseudo-communicative" legal-discursive shibboleths like "managerial discretion" (used by the majority in the Supreme Court's decision in *Garcetti v. Ceballos*) as "passwords," securing the political attention of a social group—in *Garcetti v. Ceballos,* a business elite—attentive to connotations they carry that may not be recognizable to others ("Shibboleths and *Ceballos*," 1584–85). Nagai also describes the shibboleth as functioning as a password, albeit in a "dreamy" sense ("Dream Shibboleth," 425).

71 Marcus, "Ridiculing the Ephraimites," 100.

72 Casual references to "Ali Baba's cave" are frequent in technical literature on authentication. For a more sophisticated engagement with variations on the story, see, for example, Gibson and Laporte, "Ali Baba's Cave," involving a variation on a variation by Jean-Jacques Quisquater et al. See Quisquater et al., "How to Explain Zero-Knowledge Protocols to Your Children." See also De Gregorio, "Ali Baba, Waldo and the Dining Cryptographers."

73 Todorov, "Narrative-Men," 69.

74 Peiser, "'Sesam, thue dich auf," 282.

75 Ibid., 284–85.

76 Haupt, "Open Sesame," 165–67.

77 Ibid., 170–72.

78 See especially de Man, "The Return to Philology"; Said, "The Return to Philology"; Holquist, "Erich Auerbach and the Fate of Philology Today"; Holquist, "The Place of Philology in an Age of World Literature"; Holquist, "Why We Should Remember Philology"; and Mufti, "Orientalism and the Institution of World Literatures."

79 In *Orientalism*, Said addresses the non-Orientalist "project of revitalizing philology," 258; and the "new eccentricity in Orientalism" introduced by its US Americanization (261, 290).

80 See ibid., 131–32, and Harpham, "Roots, Races, and the Return to Philology," 40–41.

81 See Lerer, *Error and the Academic Self,* 219 (on Harry Caplan), and 230 (on Erich Auerbach). Responding to Lerer's discussion of the work of Harry Caplan, Jan Ziolkowski asks, "What is the point in critiquing Harry Caplan for believing that . . . 'this whole process . . . is not about indeterminacy but about security?' Caplan was not a deconstructionist or even a poststructuralist *avant la lettre* (or *la parole*). So what? Is it not being a trifle totalitarian, to say nothing of being passé, to insist that the only certainty is indeterminacy?" (Ziolkowski, "Metaphilology," 269 [quoting Lerer, *Error and the Academic Self*, 219]).

82 See Judy, *(Dis)forming the American Canon,* 17.

83 "Subsequent to the French defeat in [the Franco-Prussian War]," Veggian writes, "the French Black Chamber, the *Bureau du Chiffre* . . . became the most effective and highly organized intelligence institution among those of the modern nations. . . . In the United States in particular, the adoption and growth of the French institutional model was accelerated in a unique manner during WWI by a group of literary scholars who had been trained in or against the methods of the anti-Shakespearean Baconists" (Veggian, "Mercury of the Waves," xxxvi).

84 Veggian, "Mercury of the Waves," xxxvii–xxxviii.

Works Cited

Arends, J. Frederik M. "From Homer to Hobbes and Beyond—Aspects of 'Security' in the European Tradition." In *Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century,* vol. 3, edited by Hans Günter Brauch, Úrsula Oswald Spring, Czeslaw Mesjasz, John Grin, Pál Dunay, Navnita Chadha Behera, Béchir Chourou, Patricia Kameri-Mbote, and P. H. Liotta, 263–77. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

Bal, Mieke. *Death and Dissymmetry: The Politics of Coherence in the Book of Judges.* Chicago: University of Chicago Press, 1988.

Baudrillard, Jean. *Passwords.* Translated by Chris Turner. London: Verso, 2011. Originally published as *Mots de passe* (Paris: Pauvert, 2000).

Beeston, A. F. L. "Hebrew *Šibbolet* and *Šobel*." *Journal of Semitic Studies* 24, no. 2 (1979): 175–77.

Bell, David Elliott, and Leonard J. LaPadula. *Secure Computer Systems: Mathematical Foundations.* Prepared for the United States Air Force, Electronic Systems Division (Bedford, MA) by the MITRE Corporation, November 1973. http://www.dtic.mil/dtic/tr/fulltext/u2/770768.pdf.

——. *Secure Computer System: Unified Exposition and Multics Interpretation.* Prepared for the United States Air Force, Electronic Systems Division (Bedford, MA) by the MITRE Corporation, March 1976. http://csrc.nist.gov/publications/history/bell76.pdf.

Brenner, Susan W. "History of Computer Crime." In de Leeuw and Bergstra, *The History of Information Security*, 705–21.

Brettler, Marc. "The Book of Judges: Literature as Politics." *Journal of Biblical Literature* 108, no. 3 (1989): 395–418.

Carnes, Pack. "'Then Say *Shibboleth*': Language Stereotyping in 'Neck-Legends.'" *Midwestern Folklore* 15, no. 1 (1989): 15–24.

Cramer, A. M. "Shibboleth." *Notes and Queries,* tenth series, 11, no. 263 (1909): 36.

Czempiel, Ernst-Otto. *Das amerikanische Sicherheitssystem 1945–1949.* Berlin: Walter de Gruyter, 1966.

De Gregorio, Alfonso. "Ali Baba, Waldo and the Dining Cryptographers." *Plaintext* (blog). November 10, 2010. http://blog.secyoure.com/en/article/354/ali-baba-waldo-and-the-dining-cryptographers.

de Leeuw, Karl, and Jan Bergstra, eds. *The History of Information Security: A Comprehensive Handbook.* Amsterdam: Elsevier, 2007.

de Man, Paul. "The Return to Philology." In *The Resistance to Theory*, 21–26. Minneapolis: University of Minnesota Press, 1986.

Derrida, Jacques. "Shibboleth: For Paul Celan." Translated by Joshua Wilner. In *Word Traces: Readings of Paul Celan*, edited by Aris Fioretos, 3–72. Baltimore: Johns Hopkins University Press, 1994.

Eco, Umberto. *The Search for the Perfect Language.* Translated by James Fentress. Oxford: Blackwell, 1995.

Etcheson, Nicole. *Bleeding Kansas: Contested Liberty in the Civil War Era.* Lawrence: University Press of Kansas, 2004.

Faber, Alice. "Second Harvest: *šibbōlɛθ* Revisited (Yet Again)." *Journal of Semitic Studies* 37, no. 1 (1992): 1–10.

Gaster, Theodor Herzl. *Myth, Legend, and Custom in the Old Testament: A Comparative Study with Chapters from Sir James G. Frazer's "Folklore in the Old Testament."* New York: Harper and Row, 1969.

Geoghegan, Bernard Dionysius. "Agents of History: Autonomous Agents and Crypto-Intelligence." *Interaction Studies* 9, no. 3 (2008): 403–14.

——. "From Information Theory to French Theory: Jakobson, Lévi-Strauss, and the Cybernetic Apparatus." *Critical Inquiry* 38, no. 1 (2011): 96–126.

Gibson, Steve, and Leo Laporte. *Ali Baba's Cave. Security Now*, episode 363. August 1, 2012. https://www.youtube.com/watch?v=xZwdwW8UacQ.

Harpham, Geoffrey Galt. "Roots, Races, and the Return to Philology." *Representations* 106, no. 1 (2009): 34–62.

Haupt, Paul. "Open Sesame." *Beiträge zur assyriologie und semitischen sprachwissenschaft* 10, no. 2 (1927): 165–74.

Hendel, Ronald S. "Sibilants and *Šibbōlet* (Judges 12:6)." *Bulletin of the American Schools of Oriental Research*, 301 (1996): 69–75.

Hess, Ken. "2012: The Year of Security." *ZDNet.* January 3, 2012. http://www.zdnet.com/article/2012-the-year-of-security/.

Higgs, Edward. "From Frankpledge to Chip and PIN: Identification and Identity in England, 1475–2005." In de Leeuw and Bergstra, *The History of Information Security*, 243–62.

Holquist, Michael. "Erich Auerbach and the Fate of Philology Today." *Poetics Today* 20, no. 1 (1999): 77–91.

——. "The Place of Philology in an Age of World Literature." *Neohelicon* 38, no. 2 (2011): 267–87.

——. "Why We Should Remember Philology." *Profession* 2002, no. 1 (2002): 72–79.

Honan, Mat. "It's Time to Abandon Passwords." *io9* (blog). June 17, 2011. http://io9.com/5812685/its-time-to-abandon-passwords.

Ifukor, Presley A. "Spelling and Simulated Shibboleths in Nigerian Computer-Mediated Communication." *English Today* 27, no. 3 (2011): 35–42.

Johnston, John. *The Allure of Machinic Life: Cybernetics, Artificial Life, and the New AI.* Cambridge: MIT Press, 2010.

Judy, Ronald A. T. *(Dis)forming the American Canon: African-Arabic Slave Narratives and the Vernacular.* Minneapolis: University of Minnesota Press, 1993.

Kaufmann, Franz-Xaver. *Sicherheit als soziologisches und sozialpolitisches Problem: Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften.* Stuttgart: Enke, 1973.

Kniffka, Hannes. "Shibboleths: Philologische Bestandsaufnahme und Gesichtspunkte zu ihrer soziolinguistischen Analyse." *Deutsche Sprache* 19, no. 2 (1991): 159–77.

Lerer, Seth. *Error and the Academic Self: The Scholarly Imagination, Medieval to Modern.* New York: Columbia University Press, 2002.

Liu, Lydia H. *The Freudian Robot: Digital Media and the Future of the Unconscious.* Chicago: University of Chicago Press, 2010.

Marcus, David. "Ridiculing the Ephraimites: The Shibboleth Incident (Judges 12:6)." *MAARAV: A Journal for the Study of the Northwest Semitic Languages and Literatures* 8 (1992): 95–105.

Marcus, Ralph. "The Word *Šibboleth* Again." *Bulletin of the American Schools of Oriental Research*, 87 (1942): 39.

McNamara, Tim. "21st Century Shibboleth: Language Tests, Identity and Intergroup Conflict." *Language Policy* 4, no. 4 (2005): 351–70.

Merrin, William. *Baudrillard and the Media: A Critical Introduction.* Malden, MA: Polity, 2005.

Michael, Jennifer. "(Ad)Dressing Shibboleths: Costume and Community in the South of France." *The Journal of American Folklore* 111, no. 440 (1998): 146–72.

Moore, George Foot. *A Critical and Exegetical Commentary on Judges.* New York: Scribner, 1895.

Mufti, Aamir R. "Orientalism and the Institution of World Literatures." *Critical Inquiry* 36, no. 3 (2010): 458–93.

Nagai, Kaori. "Dream Shibboleth." *Journal of European Studies* 38, no. 4 (2008): 421–30.

Needleman, Mark. "The Shibboleth Authentication/Authorization System." *Serials Review* 30, no. 3 (2004): 252–53.

Newman, Jared. "The Username/Password System Is Broken: Here Are Some Ideas for Fixing It." *Time.* August 8, 2012. http://techland.time.com/2012/08/08/online-passwords-are-a-broken-system-here-are-some-ways-to-fix-it/.

Niditch, Susan. *Judges: A Commentary*. Louisville, KY: Westminster John Knox Press, 2008.

Noyes, Dorothy. "Group." *The Journal of American Folklore* 108, no. 430 (1995): 449–78.

Peiser, F. E. "'Sesam, thue dich auf." *Orientalistische Litteratur-Zeitung* 1902, no. 7 (1902): 282–85.

Quisquater, Jean-Jacques, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, and Thomas A. Berson. "How to Explain Zero-Knowledge Protocols to Your Children." *Advances in Cryptology* 435. CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, CA, August 20–24, 1989 (1990): 628–31.

Rendsburg, Gary A. "The Ammonite Phoneme /T/." *Bulletin of the American Schools of Oriental Research*, 269 (1988): 73–79.

——. "More on Hebrew *Šibbōlet*." *Journal of Semitic Studies* 33, no. 2 (1988): 255–58.

Said, Edward W. *Orientalism.* New York: Vintage Books, 2003.

——. "The Return to Philology." In *Humanism and Democratic* Criticism, 57–84. New York: Columbia University Press, 2004.

Schell, Karel Johan. "History of Document Security." In de Leeuw and Bergstra, *The History of Information Security*, 197–241.

Schrimm-Heins, Andrea. "Gewißheit und Sicherheit: Geschichte und Bedeutungswandel der Begriffe certitudo und securitas." *Archiv für Begriffsgeschichte* 35 (1992): 115–213.

Sismondi, Jean-Charles-Léonard Simonde de. *A History of the Italian Republics: Being a View of the Origin, Progress and Fall of Italian Freedom.* London: Longman, Brown, Green, and Longmans, 1832.

Smith, Richard E. *Authentication: From Passwords to Public Keys.* Boston: Addison-Wesley, 2002.

Soggin, J. Alberto. *Judges, a Commentary.* Translated by John Bowden. London: SCM Press, 1987.

Speiser, E. A. "The Shibboleth Incident (Judges 12:6)." *Bulletin of the American Schools of Oriental Research*, 85 (1942): 10–13.

Stross, Randall. "Goodbye, Passwords. You Aren't a Good Defense." *New York Times.* August 9, 2008. http://www.nytimes.com/2008/08/10/technology/10digi.html?_r=0.

Stuart, Susan. "Shibboleths and *Ceballos*: Eroding Constitutional Rights through Pseudocommunication." *Brigham Young University Law Review* 2008, no. 5 (2008): 1545–601.

Swiggers, Pierre. "The Word *Šibbōlet* in Jud. xii.6." *Journal of Semitic Studies* 26, no. 2 (1981): 205–7.

Terdiman, Richard. "Taking Time: Temporal Representations and Cultural Politics." In *Given World and Time: Temporalities in Context*, edited by Tyrus Miller, 131–44. Budapest: Central European University Press, 2008.

Todorov, Tzvetan. "Narrative-Men." In *The Poetics of Prose*, translated by Richard Howard, 66–79. Ithaca: Cornell University Press, 1977.

van Biene-Hershey, Margaret. "IT Security and IT Auditing between 1960 and 2000." In de Leeuw and Bergstra, *The History of Information Security*, 655–80.

Veggian, Henry. "Mercury of the Waves: Modern Cryptology and U.S. Literature." PhD diss., University of Pittsburgh, 2005.

Warner, Michael. "Cybersecurity: A Pre-history." *Intelligence and National Security* 27, no. 5 (2012): 781–99.

Wayman, James L. "The Scientific Development of Biometrics over the Last 40 Years." In de Leeuw and Bergstra, *The History of Information Security*, 263–74.

Wisse, Pieter. "Semiotics of Identity Management." In de Leeuw and Bergstra, *The History of Information Security*, 167–96.

Woodhouse, Robert. "The Biblical Shibboleth Story in the Light of Late Egyptian Perceptions of Semitic Sibilants: Reconciling Divergent Views." *Journal of the American Oriental Society* 123, no. 2 (2003): 271–89.

——. "Hebrew *šibbōlet* 'Ear of Grain; (Olive) Branch' and 'Stream, Torrent, Flood': An Etymological Appraisal." *Studia Etymologica Cracoviensia* 7 (2002): 173–89.

Yost, Jeffrey R. "A History of Computer Security Standards." In de Leeuw and Bergstra, *The History of Information Security,* 595–621.

Ziolkowski, Jan M. "Metaphilology." *The Journal of English and Germanic Philology* 104, no. 2 (2005): 239–72.