Center for Internet and Society
at Stanford Law School

Berkman | The Berkman Center for Internet & Society
at Harvard Law School

Research Publication No. 2006-01
September 2005

Identity Management as a Cybersecurity Case Study

Presented at the

Oxford Internet Institute Conference –
Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities

Mary Rundle and Ben Laurie

JEL Classification: K330, O330, O380

IDENTITY MANAGEMENT AS A CYBERSECURITY CASE STUDY

Mary Rundle and Ben Laurie *

ABSTRACT

In our increasingly networked world, information relating to an individual is of interest for its commercial value and for its potential to help promote a safe electronic realm, among other things. In the area of commerce, there are markets demanding the collection of personal data, and at the same time there are markets demanding the protection of that data. Likewise, in the field of public safety, some international agreements provide for the monitoring of individuals, while others call for the protection of their privacy. In the midst of these tensions, new technological tools are emerging to allow increased control over personal data. It is unclear, however, how these digital identity management tools will be used, and what their deployment will mean for the individual.

This paper explores the intersection of international law and technology in the area of digital identity management. First the paper highlights provisions in international treaties and guidelines that have identity management dimensions. Next it provides an overview and technological critique of a new system for digital identity management that the Microsoft Corporation is pushing. Finally, after signaling some ambiguities regarding the interplay of the international rules and the metasystem, the paper offers some suggestions for enhancing accountability to the public.

Keywords: identity management, cybersecurity, personal data, Microsoft

* This paper has been produced under Net Dialogue, a project funded by the Lynde and Harry Bradley Foundation and jointly sponsored by the Berkman Center for Internet and Society (Berkman Center) at Harvard Law School and the Center for Internet and Society (CIS) at Stanford Law School. Mary Rundle is a Fellow at the Berkman Center and a Non-Resident Fellow at CIS. Ben Laurie is Director of Security of The Bunker Secure Hosting, a founding director of The Apache Software Foundation and a core team member of OpenSSL. The authors would like to thank Derek Bambauer, Stefan Brands, John Clippinger, Bill McGeveran, Paul Trevithick, and David Weinberger for their help in writing this piece.

IDENTITY MANAGEMENT AS A CYBERSECURITY CASE STUDY

Mary Rundle and Ben Laurie

Table of Contents

Introduction

As the Internet has become integral to the basic functioning of industrialized societies, so has cybersecurity become central to general security. However, the players involved in ensuring a secure cyberspace – that is, governments and private enterprises – may have different interests: One government's preferred order is anathema to another, and a business must strive to profit its own shareholders rather than the public at large.

Hence, in the rush to secure cyberspace, a fundamental question remains unanswered: What, exactly, are we protecting?

Defining the object of cybersecurity at the outset is critical, for this definition will set the parameters for the laws and technologies that will implement the security system. In this early stage of design, there is a window of opportunity to affect the assumptions upon which the cybersecurity framework is based. If democracy is the ideal, cybersecurity should reflect this highest value.

This paper focuses on digital identity management[1] as an element of cybersecurity to demonstrate these dynamics. This topic represents an area where significant changes are taking place on both the technological and the international policymaking fronts. As such, it offers good ground for testing how decision-makers in the technology industry and in intergovernmental organizations might come together to discuss the implications of developments in their fields, and how an interdisciplinary approach might bolster democratic mechanisms in the networked world.

Paper sections include a sampling of international initiatives with identity management dimensions; an overview of emerging identity management technology; an illustrative list of ambiguities as to how the rules and technology will reinforce each other; and reference points for designing an identity management system that encourages accountability to the public.

International Initiatives with Identity Management Dimensions

Due to the global nature of the Internet, governments are grappling at the international level to iron out cybersecurity arrangements. Negotiating in intergovernmental organizations, diplomats are crafting rules to cover a span of strategic issues for the networked world, including cybercrime, taxation, travel, money transfers, and the environment. Through clauses on identity management, recent treaties and guidelines provide governments with expanded reach over citizens.

Sampling of International Instruments

To lend a sense of the breadth of this reach, this section highlights a few of these instruments.[2]

- Convention on Cybercrime – *an initiative by the Council of Europe*

Negotiators began drafting the Convention on Cybercrime in 1992, and with its conclusion in 2001, this treaty became "the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography

[1] By "digital identity" or "identity", this paper means a digital description of a person, or "subject"; by "management", this paper means the administration of authentication, access restrictions, passwords, access rights, account profiles, and other points of control for that identity.

[2] For summaries of these instruments and others, as well as overviews of the intergovernmental organizations responsible for them, see <http://www.netdialogue.org>.

and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception."[3]

Signatories have committed to using common definitions of what constitutes cybercrime, as well as common procedures for criminal enforcement. They have also agreed to establish a "fast and effective regime" for international cooperation.

The treaty also calls on each signatory to adopt measures necessary "to empower its competent authorities to order… a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control."[4]

While comprehending that threats could be grave, the drafters were nonetheless careful to limit the use of the new powers and procedures to specific criminal investigations or proceedings, rather than extending them to communications generally.

- Biometrics in Machine-Readable Travel Documents – *an initiative by the International Civil Aviation Organization*

The International Civil Aviation Organization (ICAO) in 1997 began developing "a global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents…"[5] ICAO members adopted this blueprint in 2003. Although implementation is a tall order, ICAO has a full program underway to achieve this harmonization.

Countries that are members of ICAO are arguably obliged to go along with this global system of electronic travel documents: Article 22 of the Chicago Convention charter requires signatories to "adopt all practicable measures... to prevent unnecessary delays to aircraft, crews, passengers and cargo, especially in the administration of laws relating to immigration, quarantine, customs and clearance."

ICAO has stated that the "blueprint, set out in technical reports and specifications, will assist all 188 Member States to implement a worldwide, standardized system of identity confirmation."[6]

- Electronic Commerce Taxation Framework Conditions – *an initiative by the Organization for Economic Cooperation and Development*

E-commerce naturally piques the interest of revenue authorities responsible for collecting the taxes that foot the bill for security and other government expenditures. Taxation of cross-border e-commerce requires coordination among different countries' tax authorities. To begin defining elements of a tax treaty, members of the Organization for Economic Cooperation and Development (OECD) in 1998 agreed on Electronic Commerce Taxation Framework Conditions that they had begun drafting the previous year. The Framework sets out the broad goals of supporting neutrality, efficiency, certainty, simplicity, effectiveness, and fairness in the taxation of e-commerce.

---

[3] Council of Europe, *Convention on Cybercrime*, CET 185, November 23, 2001. Signatories include 38 European countries plus Canada, Japan, South Africa and the United States. The treaty entered into force in January 2004 once five countries had ratified it. According to the COE website (<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, as viewed on August 28, 2005), 11 signatories had ratified the Convention as of mid-2005.

[4] Article 18. That same Article defines "subscriber information" as "any information… that is held by a service provider, relating to subscribers of its services… by which can be established… the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement…"

[5] See ICAO's website at <http://www.icao.int>. For an additional overview of this organization and a summary of this initiative, see <http://www.netdialogue.org/initiatives/icaomrtd/>.

[6] ICAO Press Release dated 28 May 2003.

This OECD instrument calls for countries to "ensure that appropriate systems are in place to control and collect taxes." As part of this effort, tax revenue authorities are to "make use of the available technology and harness commercial developments in administering their tax system." By employing identity management tools, they will be living up to their pledge and will "maintain their ability to secure access to reliable and verifiable information in order to identify taxpayers and obtain the information necessary to administer their tax system."[7]

Recent proposals by an advisory group tasked with moving this agenda forward include requirements for businesses and consumers engaging in transactions to maintain records containing electronic signatures, among other elements, and to make these records available to tax authorities wishing to do audits.[8]

- Recommendations on Terrorist Financing – *an initiative by the Financial Action Task Force*

In the wake of the terrorist attacks in the United States on September 11, 2001, governments involved with the Financial Action Task Force (FATF)[9] adopted Special Recommendations on Terrorist Financing.[10] Complementing their Forty Recommendations on money laundering, these additional provisions "set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts."[11]

Recommendation VII stipulates that "countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain."

Notably, this Recommendation on wire transfers includes both domestic and cross-border transfers between financial institutions.[12] The Interpretive Note explains that this Recommendation:

> "… aims to ensure that basic information on the originator of wire transfers is immediately available (1) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals, (2) to financial intelligence units for analysing suspicious or unusual activity and disseminating it as necessary, and (3) to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions."[13]

In effect, signatory governments have assigned themselves new powers as they will have the immediate means to check who is sending money to whom. Currently they rely on the goodwill assistance of private financial institutions to implement this agreement. Once strong identity management technology is built into the Net, governments will be equipped to enforce these regulations tightly.

---

[7] OECD, Electronic Commerce Taxation Framework Conditions, Section V, Box 3, October 1998.
[8] Centre for Tax Policy and Administration, Tax Guidance Series, "Transaction Information Guidance," May 4, 2005, para. 55 and Annex II.
[9] FATF members include 33 countries, listed at <http://www1.oecd.org/fatf/Members_en.htm>, as viewed on August 29, 2005.
[10] Financial Action Task Force, *Special Recommendations on Terrorist Financing*, October 31, 2001, with an additional recommendation added in 2004.
[11] *Id*., Preamble.
[12] Financial Action Task Force, *Revised Interpretive Note to Special Recommendation VII: Wire Transfers*, para. 3.
[13] *Id.*, para. 1.

- Global Earth Observation System of Systems – *an initiative by the Group on Earth Observations*

The intergovernmental Group on Earth Observations (GEO)[14] was established in 2003 with a mandate to "improve coordination of strategies and systems for observations of the Earth and identify measures to minimize data gaps, with a view to moving toward a comprehensive, coordinated, and sustained Earth observation system or systems," and to "exchange observations recorded from in situ, aircraft, and satellite networks," among other tasks.[15]

GEO adopted a 10-Year Implementation Plan for its Global Earth Observation System of Systems (GEOSS) in early 2005, instituting a major but relatively unnoticed process for tying together the globe's monitoring capacities. The expanse of this initiative is best stated in the 10-Year Implementation Plan itself: "The vision for GEOSS is to realize a future wherein decisions and actions for the benefit of humankind are informed via coordinated, comprehensive and sustained Earth observations and information."[16]

This non-binding initiative is billed as entailing global information sharing "to qualitatively improve our understanding of the Earth system, markedly enhancing global policy- and decision-making abilities to promote the environment, human health, safety, and welfare."[17] There are no prescribed limits as to what types of information will be exchanged and analyzed in this "System of Systems". Rather, this instrument leaves open the application of this combined intelligence. Examples of applications already envisioned include the tracking of "pathogen occurrences, as well as patterns of human activities," with forecasts allowing "public-service and environmental managers to modify behaviors ... to avoid exposure."[18] In other words, this mechanism could be used, for example, to monitor individuals' movements so as to identify who should be quarantined to stop the spread of contagious diseases or the effects of bioterrorism.

Notably, the instrument stipulates: "Use of data or products does not necessarily imply agreement with, or endorsement of the purpose behind the gathering of such data."[19] This language could stimulate a market in illicitly collected personal data[20]; so, too, it would seem to allow governments to circumvent limitations on "state action" if drawing on information collected by private actors. With its lofty goals but potentially more problematic implementation, this initiative is laden with underlying tensions.

Trends of Increasing Personal Data Collection

The scale of today's threats has caused governments to cooperate like never before. Looking at these initiatives chronologically, however, the trend in international arrangements seems to be for governments to capture and analyze an increasing amount and scope of information on people's behavior.

---

[14] Currently, GEO consists of 47 members and 29 participant international organizations. The GEOSS 10-Year Implementation Plan was endorsed by nearly 60 governments and the European Commission.

[15] *Declaration of the Earth Observation Summit*, Washington, DC, July 31, 2003. "In situ" connotes measurements taken through direct physical contact; other mechanisms covered by the agreement entail remote measurements.

[16] Group on Earth Observations, *Global Earth Observation System of Systems: 10-Year Implementation Plan*, February 2005, p.1.

[17] *Id.*, Foreword.

[18] Group on Earth Observations, *Global Earth Observation System of Systems: 10-Year Implementation Plan – Reference Document*, February 2005, p. 45.

[19] Group on Earth Observations, *Global Earth Observation System of Systems: 10-Year Implementation Plan*, February 2005, Section 5.4.

[20] By "personal data", this paper uses the definition "any information relating to an identified or identifiable individual" as found in the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, CETS 108, adopted in 1981.

The trend may be summarized as follows:

- Instead of gathering data on suspected criminals only (e.g., cyber attackers), recent international initiatives look to collect data on average citizens (e.g., taxpayers);

- Whereas information on unusual activities used to be captured for analysis (e.g., communications related to crime), now everyday activities are under instantaneous surveillance (e.g., financial transactions over wires);

- Rather than focusing on cross-border activities alone (e.g., foreign travel), international provisions now extend to people's activities in their home countries (e.g., location tracking for gauging exposure to contagions).

Will this trend continue?

Identity Management from an Industry Vantage Point

While governments have picked up on the advantages of monitoring the public to help crack down on "big picture" problems like network attacks, terrorist travel, tax evasion, money laundering, and the spread of pathogens, the technology industry has been developing identity management solutions in response to market demand.

Waning Public Confidence in the Internet and Microsoft to the Rescue

The signal that the market is giving to the technology industry is a growing reluctance of society to trust the Internet, given today's sustained, organized, and increasingly sophisticated cyber attacks (e.g., phishing, pharming, and data loss[21]). Statistics published in mid-2005 showed a sharp drop (42%) in the number of consumers who feel comfortable participating in e-commerce, as well as a large decline (28%) in the number of people who feel safe engaging in Internet banking.[22]

The public holds a general, fuzzy view that somehow Microsoft is to blame for the rising number of cyber attacks. The perception is that since countless people use Microsoft Windows, and since these same people find themselves subject to cyber attack, there must be a correlation, and Microsoft should shoulder the responsibility of doing something about it.

Microsoft, meanwhile, has learned from past experience[23] that people do not want the company to be at the center of their trust relationships or to occupy a monopoly position in identity management. Therefore, to respond to today's authentication problems, Microsoft is reaching out to the technology industry to build a "metasystem" that will allow different identity management systems to interoperate – including, for example, those of Sxip, the Liberty Alliance, Shibboleth, Passel, and other industry players. These tools will eliminate the need for the user to memorize dozens of passwords and type in payment information for e-commerce transactions; they will also provide users with security as to who is on the other end of a transaction.

---

[21] As described by David Bank and Riva Richmond, "Information Security: Where the Dangers Are," Wall Street Journal, July 18, 2005: "In 'phishing' scams, fraudsters send emails that appear to come from a trusted source, like Citibank or eBay. Click on a link in the email, and you're directed to a fake Web site, where you're asked to reveal account numbers, passwords and other private information… Then there's 'pharming,' where hackers attack the server computers where legitimate Web sites are housed. Type in the address of the legitimate site, and you are redirected to a look-alike."

[22] Riva Richmond, "Internet Scams, Breaches Drive Buyers Off the Web, Survey Finds," Wall Street Journal, June 23, 2005, p. B3, reporting on a Gartner study of 5000 online consumers.

[23] In the past several years the market has largely rejected Microsoft's "Passport" identity management system for cases in which Microsoft had no direct role as a party in the transactions.

Widespread use of this metasystem is likely based on Microsoft's position: Microsoft has its own identity management services that will work with this general metasystem. The company is on the private campaign trail to convince big e-commerce players like Amazon and eBay to accept these new services in exchange for more direct access to Microsoft customers. Microsoft will introduce these services not only in its next version of Windows, called "Windows Vista"[24] (scheduled to be released in 2006), but also in upgrades for users of a current version of Windows, i.e. Windows XP. Because so many people use Windows XP, the spread of these services operating with the metasystem will be independent of Windows Vista adoption rates. With a spur like this, the metasystem has a strong probability of taking root.

The Basics of the Identity Management "Metasystem"

Identity management is not a new notion. Indeed, there have been many attempts to establish methods for people to authenticate themselves and ascertain the identities of those with whom they are dealing online. Rather than trying to replace all these systems, the "metasystem" aims to allow them all to interoperate. As described in a Microsoft paper[25], "The metasystem enables identities provided by one identity system technology to be used within systems based on different technologies, provided an intermediary exists that understands both technologies and is willing and trusted to do the needed translations."

This metasystem has two main parts: One handles the exchange of identity information as it passes *between* endpoint computers or devices, and the other helps a user manage his identity information *on* his computer. For the part between devices, the metasystem may be thought of as a set of communications standards[26] (called computer protocols) that govern the exchange of identity information in the form of packaged, sealed "digital identities", often called "tokens". Different "identity providers" may do the packaging, putting into the token the required set of "claims", or pieces of information that it attests to (e.g., that person's address, Social Security number, etc.). With the metasystem, the user can choose whatever identity provider he wants to guarantee his information and package it into secure tokens, even employing different identity providers for different purposes (e.g., one to handle core personal information like name and date of birth, another to handle credit card information such as the number and expiration date and the cardholder's name and address; another to handle medical records such as immunizations, allergies, family health history; etc.). The identity provider may reside on a person's computer or device, though in most cases it will be located elsewhere, accessible through the Internet.

So, for example, when parties interacting online need to verify information about each other, the computer or device on one end (in computer security parlance, the "relying party") will indicate to the computer or device on the other end (the user-controlled "agent") what package of information is needed. The agent will request the appropriate token from one or more identity providers entrusted with this information and pass this token to the relying party. The user can supervise this exchange on a case by case basis, or he can choose in advance to let the exchange take place automatically.

The other part of the metasystem is what happens on a person's computer or device, for example on his Windows desktop. Instead of typing in passwords or filling in an array of fields as users do today when transacting online, a person will simply choose among a visual representation of his various digital identity tokens (which Microsoft calls "InfoCards") that will contain the type of information needed (e.g., banking, medical, or tax information). In the same way that a person currently carries various cards in his wallet, such as a driver's license, an affiliation membership card, a credit card, etc., the InfoCards may be

[24] While under development the "Windows Vista" operating system has been called "Longhorn."

[25] *Microsoft's Vision for an Identity Metasystem*, May 2005, as viewed on August 29, 2005 at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/identitymetasystem.asp>.

[26] A consortium involving Microsoft, IBM, and other technology firms developed the standards for this exchange as part of a larger set of standards for web services.

thought of as a digital collection of cards that are accessible to the user for various purposes. When the user chooses the visual representation of an InfoCard for a given transaction, his agent releases the corresponding digital tokens issued by identity providers to the relying party, as described above.

This agent would be able to operate on all sorts of devices, be they desktop computers or cell phones or other mobile devices. It would be the sole component of the metasystem with which the user would need to authenticate himself directly (e.g., through a fingerprint or iris scan).

Better User Control over Personal Data

For the user to have effective control over his various digital identities, an identity management system would need certain key properties. These properties are described in the text box on the next page.

Three Key Properties of an Identity Management System

First, the information presented should be *minimal* – that is, only exactly what the relying party needs to know about the user should be revealed by the agent, and no more. For example, as mentioned above, if the relying party needs to know that I am over 21, then that is what should be revealed, not my date of birth. Or if the relying party needs to know that I am a member of some club (customers of a particular bank, for example) then what should be disclosed is just that fact, not *which* member of the club I am.

Second, presentations of information should be *unlinkable*. That is, if I go to a website today and prove I'm over 21, and then go to the same website tomorrow and prove it again, the website should not be able to link those two events together to know it was the same user that made the two proofs.[27] Unlinkability should also be in effect when proving different information, or going to different relying parties. This feature prevents the relying party (or a group of parties) from gathering information a piece at a time until my entire profile has been revealed and is then available on each future interaction, regardless of what I intend to disclose at that time.

Third, the information should be *verifiable*. It isn't good enough for me to simply state "I am over 21, trust me" – the fact must be presented such that the relying party can confirm that a trusted entity has made this assertion.

Existing widely used identity mechanisms provide us with this third property, verifiability, but not the other two features. This is because, in general, these mechanisms consist of a *certificate* – that is, a collection of statements about the user together with a *signature* on those statements. When a user wants to prove a fact about himself, he has no option but to present the whole of the certificate – since the signature is tied to the entire certificate rather than to its individual elements. This bundling, of course, immediately breaks both the minimality and the unlinkability requirements (as the certificate provides more information than necessary and as the numerous pieces of data appearing together allow a person to be pinpointed).[28]

[27] A proof is a means by which one party demonstrates to another the truth of a statement.

[28] The system could mitigate this problem to some extent by producing a separate certificate for each claim, with that claim containing the minimal set of information, but this still leaves two problems: first, each showing of any

If you wanted to leverage existing systems but still provide these three properties (as Microsoft, IBM, Sxip, and other industry players would like to do), then you end up having to generate certificates on-the-fly. Since the certificates must still be signed by the appropriate identity provider, this means the agent ends up being in the middle of a three-way conversation involving the relying party, the user, and the identity provider: First the relying party tells the agent what claims it needs; then the agent consults the user (or the user's predefined choices) and chooses the identity provider(s) for the required claims; and finally the agent goes to the identity provider(s) and requests a single-use certificate with *just these claims*. (In this last step, the agent will have to prove the validity of the user's claim to the identity provider – i.e. the agent will need to show that it has in fact been designated as an agent by the user, and that the user is who he says he is – so that the identity provider is able, in good conscience, to produce the appropriate single-use certificate.)

Because the metasystem will involve using certificates that do not have the minimality and unlinkability properties,[29] one will have to hope that the identity provider does not collude with the relying parties to reveal further information to them – an act which could be done trivially. (For example, the relying party might ask the identity provider, "Who did you give this 'over 21' certificate to?" and the identity provider could recognize it from, say, the timestamp.)

Another risk inherent in this approach is that a small number of identity providers could end up owning the market for these minimal certificates: once these three-way protocols have been introduced, it becomes easy for the relying party to say it will accept certificates from a select group of identity providers, who can then issue proxy certificates for the wider universe of identity providers that offer services to the user. [30] (For example, Verisign could get into the business of signing minimal certificates that say, in effect, "The UK Government says he's over 18," so that relying parties can delegate their trust decisions to Verisign. Verisign does the checking of the original certificate and then issues its own certificate.) Presumably, this smaller set of trusted authenticators could then have control over vast amounts of personal data; while they may offer valuable services derived from this data (e.g., targeting users with ads that are tailored to their interests), this new level of concentration could be deficient in its accountability to users and society generally.[31]

---

particular claim would be linkable, and second, it is difficult to provide general-purpose minimality since anticipating the minimal answer to every possible query ("show that either you are a UK citizen and over 21, or you are Brazilian and over 18"), and creating a fixed collection of claims encompassing each of these variations are both challenging. These problems can be solved with a class of proof known as a "selective disclosure proof," which allows the prover to prove some property of a fact to the authenticator without revealing exactly what that fact is. (For example, a person could prove that he was credit worthy without actually revealing his financial history.) Unfortunately, selective disclosure proofs are not widely used, or even understood. (Of course, governments could change this situation by including these specifications in procurement contracts.) See Stefan Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*, MIT Press: 2000 (downloadable at <http://www.credentica.com/the_mit_pressbook.php>). See also Endre Bangerter, Jan Camenisch, and Anna Lysyanskaya, "A Cryptographic Framework for the Controlled Release of Certified Data," at <http://www.prime-project.eu.org/public/prime_products/papers/Scienpapers/bacaly04.pdf>.

[29] As discussed above, one objective of the metasystem is to allow existing certificate systems to work with it, and these do not have the properties of minimality and unlinkability.

[30] There is a standard trade-off here: is it better to have one trusted identity provider and monitor it rigorously, or to allow competition and risk having dodgy entities set up their own certification authorities?

[31] As mentioned in footnote 28, selective disclosure proofs can solve all of these problems; however, in order to do so, they rely on a property we do not currently have: untraceability of the underlying network. Even if I have a system that provides perfect unlinkability at the certificate level, I lose it at the network level in today's systems: the IP address I connect from, the cookies I have in my browser and all sorts of other little clues make my various visits to sites linkable, and therefore defeat the whole purpose of careful identity management. This leads to the rarely recognized fact that, to allow the user to maintain control over information relating to himself, the network itself needs to provide anonymity as a *minimum* requirement. Although this anonymity is possible to achieve today (for example, using Tor -- see <http://tor.eff.org/>), it is not particularly easy and results in considerably reduced

Given this current arrangement versus the ideal scenario where information presented is minimal, unlinkable, and verifiable, it may seem that there is an "either/or" dichotomy – where the limitations of existing, already deployed identity schemes would mean that an identity management system would either have to start all over again to enable the user truly to manage his digital identity, or the system would have to deviate from the idealized model presented above to accommodate systems that are already in use. The practicality is that for a system to take root, it would have to grandfather existing systems; over time, however, the market may gravitate toward models that provide greater user control.

Moving Forward Just the Same

If the plans of Microsoft, IBM, and others succeed, the metasystem's tokens will be accepted in the near term as standard currency in identity management. E-commerce will be easier and more secure, and problems like phishing, pharming, and spam will diminish. As such, the identity metasystem will have succeeded in addressing the problems of today that threaten the public's confidence in the Internet.

Again, at the core of this metasystem, making it viable, is the basic authentication between the user and his agent, upon which all other claims transfers will be based.

Ambiguities as to How the International Rules and Technology Will Interact

Arguably, the identity management approaches by government and the private sector represent two sides of the same coin: that is, they both aim to provide security and convenience, with authentication of the individual being the crux. What is striking is the degree to which the international rules and technology may combine to enable comprehensive surveillance in the networked world.

As noted above, the most crucial step in the metasystem hinges on the initial authentication between the user and his agent, upon which all other claims transfers are then based. It is quite conceivable that the universal biometric standards in ICAO's Machine Readable Travel Documents could become the global mechanism for government-sanctioned proof of identity. This internationally recognized electronic identity would then serve as the ultimate guarantor that a person is who he says he is and that claims transfers based on that identity are valid. With such order, online activity could thrive. Of course, on the flip side, the identity trail left by claims transfers in the metasystem could cause individuals to be monitored far beyond what the endorsers of the ICAO rules envisioned.

With data on individuals readily available, enforcement agencies could more easily comply with the specificity requirements of the Cybercrime Convention and seek greater information from Internet service providers (ISPs). To the degree that electronic identities are included with addressing data, it is foreseeable that governments would want regular access to more data for fighting crime (e.g., as part of an effort to curtail spam, denial of service attacks, and other menaces). Again, although cybercrime poses a serious threat, the technology may give governments a larger capacity to monitor people's associations and communication patterns than originally conceived.

Similarly, this fusion of governmental and private approaches to identity management should enable governments to enforce FATF provisions that require financial institutions to verify and record identities associated with funds transfers.[32] With a system of irrefutable electronic identities, people will be far less

---

functionality. There is also the social stigma involved: Despite the perfectly legitimate need for anonymity, it is often thought that only those with criminal intent would want to use it.

[32] Policymakers already anticipate that these "documents" could have other uses, as suggested in an April 2005 panel discussion before the Computers, Freedom and Privacy Conference, when Frank Moss, Deputy Assistant Secretary for Passport Services of the Bureau of Consular Affairs, U.S. Department of State, referred to possible future uses in the context of financial transactions.

able to hide money transfers even if financial institutions are willing to help them do so. Crime may drop, but will there be a chilling effect on innocent people's activities?

So, too, countries could require that the electronic signatures used in international electronic contracts be based on these government issued electronic identities. In addition to providing assurances to contracting parties, governments could push for this as a standard way to determine when taxes were due, and to which jurisdiction.[33] While promoting efficiency, fairness, and other objectives in tax administration, governments no doubt will need to be careful to avoid a certain invasiveness.

If governments required individuals to carry identification "documents" in a physical form that was readable without contact (as planned in ICAO regulations on Machine Readable Travel Documents[34]), GEO's sensors and other technologies could track movements of all individuals.[35] Again, private sector entities could be heavily involved in the provisioning of information.[36] In the abstract such super-surveillance may seem out of the question, but in the case of an outbreak like Severe Acute Respiratory Syndrome (SARS), using the "System of Systems" to chart who had been exposed to the disease – and to identify who, therefore, should be quarantined – could appear the socially responsible course of action.

Again, the agreement has no prescribed limits as to how this System of Systems might be used. Instead its 10-Year Implementation Plan heralds the arrangement's capacity to "enhance delivery of benefits to society in the following *initial* areas…" (emphasis added). The very existence of the system may tempt governments to use it as an all-purpose remedy for situations that arise. Will this extra empowerment of government or its private sector designates be met with a corresponding increase in accountability to the public?

Designing an Identity Management System that Prevents the Abuse of Power

The discussion above has shown that the combination of international rules and emerging technology in identity management may inadvertently give government and the private sector an unprecedented amount of information on individuals in the networked world. Still, while these identity management capabilities yield enormous powers, they are not in and of themselves contrary to democracy. The key is whether the system's design enables citizens to maintain authority over government (or the powers acting in

[33] If governments were directly involved in authenticating identities for e-contracts, they would be a middle party. It is easy to see why they might wish to do so (e.g., to know when transactions were taking place for tax purposes), but whether this intervention would be desirable remains another matter. Given that each user will participate in countless exchanges of information, it is simply inefficient for each agent on the end of a transaction to have to involve identity providers every time that information must be authenticated. So, for example, it would be much more efficient for a person to have control over his electronic signature than for him to have to go through an identity provider (e.g., the government) each time he wished to sign something. Like a driver's license today, the individual could hold this government issued "document" for everyday use. For a detailed discussion of the efficiencies of user-centric identity management, see Stefan Brands' blog, "The Identity Corner," at http://www.idcorner.org/. For an account of how a user-centric identity system would work in practical terms, watch David Weinberger's Supernova blogcast interview (June 22, 2005) with Dick Hardt on "What might user-focused digital identity look like?" found at <http://news.com.com/Supernova+2005+blogcast/2030-12_3-5745034.html?%20tag=nl#hardt>, as viewed on August 29, 2005.

[34] For more information, see ICAO, "Use of Contactless Integrated Circuits In Machine Readable Travel Documents," Mike Ellis, Version 3.1, April 16, 2003.

[35] Notably, the International Organization for Migration has begun to explore how to use technology to track the movements of persons.

[36] Section 5.4 of the instrument stipulates: "Use of data or products does not necessarily imply agreement with, or endorsement of the purpose behind the gathering of such data." Group on Earth Observations, *Global Earth Observation System of Systems: 10-Year Implementation Plan*, February 2005.

governmental capacities[37]) and whether the design offers an individual effective recourse when his rights are not honored.

Beyond the Collection and Analysis of Personal Data

Of course, people tend to associate the collection and analysis of personal data with the abuse of power. A few examples from last century demonstrate this relationship: The regimes of Stalin, Hitler, and Mao had certain elements in common – that is, they all collected information on people and kept it in secret dossiers. This lack of transparency created a sense of helplessness, paranoia, and conformity in their societies and allowed these rulers to seize totalitarian power.

By contrast, other societies have been subjected to similar secret file keeping and have managed to correct power abuses – for example the United States during McCarthyism or Switzerland in the 1980s, when it was discovered that government officials had been keeping extensive dossiers on citizens. Why were these societies able to turn the situation around? Were there certain factors in the structure of their systems that made the difference? Are there lessons for identity management in the networked world?

To counteract the possibility of personal data being mishandled in the information age, the OECD and the Council of Europe (COE) each developed rules more than two decades ago.[38] Together, these initiatives comprise a solid list of protections regarding personal data collection and processing. OECD principles include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. Article 6 in the COE Convention adds an anti-discrimination provision. However, the OECD rules are non-binding, and those of the COE hold only for signatories.[39]

Even if adopted on a binding basis throughout the world, these instruments are insufficient for guaranteeing the proper treatment of personal data. After all, the totalitarian regimes of the last century could still have carried out their atrocities while such principles were "on the books".

Pivotal Principles for Ensuring Accountability

Indeed, certain principles prove pivotal for ensuring government accountability to the public. Principles involve both the *structure of government* and *certain rights of citizens*. Core principles are elaborated in the boxes below.

Local Government Enabling Accountability

The principle of subsidiarity holds that decisions should be made at the most local level practicable. This idea rests on the notion that the people who are closest to a situation are the ones most able to make sound judgments relating to it. In democracy this principle is important because a democratic government is supposed to be responsive to its citizenry, and the closer this government is to its citizenry, the greater its ability to understand and respond to their needs and desires.

[37] Private sector entities can take on governmental roles – for example, providing security. To maintain democracy, therefore, citizens and not just shareholders would need to be able to hold these actors accountable, either indirectly through government supervision or more directly through some other mechanism(s).

[38] OECD members adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980. The Council of Europe adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, CETS 108, in 1981. These organizations have adopted subsequent instruments to reinforce these ideas.

[39] Signatories include 38 European countries, 33 of which have ratified the Convention.

With respect to identity management, international policymakers might argue that, for ease of administration, key personal information (such as digital representations of biometric data) should reside in centrally administered (i.e. international) databases. However, a different design could charge local repositories with holding such information, with access by central authorities permitted only according to specific procedures. By storing information closer to the people (e.g., at the national, state, or municipal level, assuming it needed to be stored at all), the system would entrust local government authorities with the relevant information, with these authorities responding to queries and releasing data only when there were good reason, according to established criteria.

But even with such an arrangement, wouldn't it still be possible for local authorities to grow corrupt? What is to prevent the controller of data from using its position to reach for more power? These questions are the subject of the box below.

Counterbalancing Government Roles

Another feature of democracy may be viewed as the citizenry granting the government limited authority and building "separation-of-powers" and "checks-and-balances" into the internal structure of government itself so that power is not used to amass more power. By intentionally pitting governmental roles against each other, the system counterbalances power-holders so that they act as checks on each other, preventing any one arm from exercising too much power.

Separation-of-powers and checks-and-balances could be built into identity management both legally and technologically. For example, if the law mandated Internet access controls, the computer code could ensure that the data controller for authentication (i.e. that which verifies a person's identity and grants clearance to use the Internet) be independent from the institution who determines when access should be restricted; meanwhile, the code could require that a third institution then vet any request to block access, checking the request against prescribed criteria and providing an opportunity for appeal.

In addition to these structural arrangements for government, proper identity management can also be ensured by watchfulness on the part of citizens. For this vehicle to be effective, of course, people need to have certain guaranteed liberties, as described in the following box.

Citizens Demanding Accountability

Other forces that act to keep power from being amassed and abused fall outside the structure of government and involve certain rights that the citizenry holds. A package of rights that enables them to respond to power abuses includes the following: (1) the right to receive and impart information (i.e. the right – including the practical means – to communicate); (2) the right to associate and assemble, which enables the formulation and expression of shared concerns, as well as the planning of appropriate responses (e.g., peaceful protests); (3) the right to hold beliefs freely; and (4) the right to enjoy privacy, which supplements these other freedoms by preventing power-holders from intimidating people who might dissent.

These principles are enshrined in the Universal Declaration on Human Rights.[40]

The right to receive and impart information could call into question restrictive controls on Internet access (e.g., requirements for proof of citizenship). Technological tools could bolster the right to receive and impart information and the right to associate and assemble, by creating an audit trail for missed attempts to communicate or meet virtually. Likewise, law and code could combine to preserve privacy by specifying legal protections for personal data and by providing electronic audit trails to verify that these protections were honored by the entities having control over information at different stages.

Conclusion

In sum, both international rules and technology point to the adoption of a global electronic identity system in the name of security and convenience. Emerging as the cumulative result of incremental pressures and responses over time, this system for international identity management has not yet enjoyed the benefit of forethought as to how law and technology will interact. Concern for democracy in its essence – that is, citizens' authority over government – must be held as paramount if this system is to achieve its potential. Likewise, the legal and technological workings of identity management must be designed with this in mind.

Most democracies have come about after a struggle against oppression, and their design thus reflects a distrust of concentrated power. So, too, the cybersecurity system should reflect this concern. Rather than the mantra, "Maintaining the safety of our society is our first priority" (as though pursuing security for its own sake), democracies would more faithfully hold up the cybersecurity banner that reads, "Maintaining the freedom of our society is our first priority."

As people present at a time of crucial decision-making for the future, we have a responsibility to use this window of opportunity to instill the early identity management system with democratic principles for the common good. By being attentive to democracy in other aspects of cybersecurity as well, we are much more likely to arrive at true security.

[40] Adopted and proclaimed by UN General Assembly resolution 217 A (III) of 10 December 1948, the *Universal Declaration on Human Rights* reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation…" (Article 12); "Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance" (Article 18); "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (Article 19); "Everyone has the right to freedom of peaceful assembly and association. No one may be compelled to belong to an association" (Article 20, paras. 1 and 2).