6 – The Accountability Component

Question 6 *We value anonymity, but at the same time we want others to be accountable. What happens when someone whose privacy is protected anonymously harms me, my community, or my country?*

Answer 6 The Accountability Component

As QEI must protect your privacy, it also must protect your right to recourse if you are harmed by someone whose privacy is similarly protected. Law enforcement must also be able to seek a court order for identity disclosure when a legitimate court deems it necessary for the protection of public safety. The Accountability Component ensures that due process prevails even in jurisdictions that are not known for adherence to due process.

Privacy for Me, Accountability for You

As we have noted, everyone wants anonymity for themselves, and everyone wants others to be accountable for their actions. We also discussed accountable anonymity, the practice of separating the credential(s) you use from your Digital Birth Certificate or other foundational certificate and the personal information in it, comparing it to the separation of automobile registration information from driver licensing information. Anyone can see your car's license plate, but others on the roadway only get to know your name and address if a right to know and a need to know are legally established, as when you've been in an accident.

The Accountability Component of the Quiet Enjoyment Infrastructure spells out the circumstances under which (to adapt a phrase from corporation law) your "veil of anonymity" can be penetrated.

Let's start with the simplest case: commenting on a blog story. You want to reply to the blogger or to other commenters in public, but you want to post under a pseudonym to avoid disclosing your identity to everyone else who reads the blog, including the bots that tirelessly harvest such information from the millions of postings on thousands of blogs.

Some bloggers permit anonymous comments provided that the commenter uses the pseudonym "Anonymous Coward," which tends to limit the number of such postings. Others require posting under a handle, which can easily be concocted and registered for the occasion. Sometimes the blogger will require the usual weak ID check, a validation message with a link or code sent to the commenter's email address—another practice that tends to limit a blog's commenting activity. And antisocial trolls tend to have an inventory of untraceable Hotmail or Ymail accounts.

The inevitable degradation of blogs by these jerks is the smaller part of the concern.

What happens when one of them defames you anonymously in public? Where do you send the cease-and-desist letter, the demand for a retraction and apology, the notice of intent to sue?

QEI's Accountability Component addresses the problem with accountable anonymity. Whether a blog is established in an indoor online space or in traditional outdoor Web space, the blogger has a number of options to choose from:

- Automatically sign a commenter's PersonalNDA and request a license to know the commenter's natural name. The commenter's natural name is then programmatically retrieved from his MOI but it is not posted with the comment. Only the blogger is licensed to have that information; the blogger may not disclose it to anyone else.
- The contingent license: Same as previous, but the license is not used and the name is not disclosed unless the blogger decides there is cause to retrieve it any time after the comment is entered.
- Require a digital signature from the PEN of a credential of minimum identity quality; the signature itself does not appear on the posting.
- Require publication of the identity quality score alongside the comment, with links that allow anyone to sign the commenter's PersonalNDA and request a license to view name, image, or other information.

Beyond blog commenting, plenty of examples can be cited where some level of explicit accountability might be needed among private parties. Operators of social networks for children need to know at least the age, gender, and Enrollment Practices score of participants, without requiring participants to identify themselves to each other. Those who provide industry portals will need a way to establish recourse when things don't go as planned among participants.

Court-Ordered Identity Disclosure

In settings where disclosure is not provided for with such contingent licensing or other previous arrangements that are built into the interaction, the Authenticity Infrastructure keeps the connection between the identity you use and the contents of your foundational certificate hidden. But the connection can be disclosed, if due process calls for it. A court order is required to compel disclosure of a subject's identity information by the Osmio Vital Records Department.

But which court? Can the City of Osmio honor any piece of paper postmarked from anywhere in the world purporting to be a court order? Just to get a handle on the scale of the challenge we sought an answer to the question, "How many bona fide courts of law are there in the world?"

An answer on Yahoo! from a lawyer in the state of Arizona in the U.S. underscores the size of the problem. "If you are asking about the first part — all the courts in Arizona — I am not sure how to find that out. Because, just about every city has a municipal court. Then, there are county courts and within the county court system there are divisions: Criminal, Civil, Juvenile, Probate. (Get the idea?)"

In its 2013 edition the *World Cities Database* provides information on 3,156,377 municipalities. If only 1 in 10 of them has a municipal court, we have over 300,000 legitimate potential sources of court orders.

And so the City of Osmio will have its own juries to judge the legitimacy of each court order. Anyone with a minimum Identity Quality score may be chosen at random to serve on a jury, which convenes only online, of course. The jury will be provided with a scanned image of the court order and any supporting information.

So much for the more or less civilized world of private-party disclosure of identity. Now let's acknowledge the elephant in the room, the Big Brother issue.

It's More about Authenticity than Confidentiality

In the latter half of 2013, Edward Snowden's disclosures have everyone talking about government intrusion on private encrypted communication. Before we get into that, keep in mind that encryption in QEI is mostly about its role in digital signatures. Encryption of files and messages is certainly enabled by the Quiet Enjoyment Infrastructure, but QEI is much more about authenticity than confidentiality.

Let's also keep in mind that our source of public authority, the City of Osmio, has nothing to do with the public authority that the U.S. National Security Agency and its partners in the governments of the U.K, France, Canada, Australia, and New Zealand wrongly or rightly claim supports their widespread interception and decryption of private communications. It's not as though we have any influence on the policy of governments other than that of Osmio.

However, QEI can inform suggested solutions to the very real and very alarming problem of a rogue government agency doing what rogue government agencies do, that is, amassing new and illegal power under the pretense of protecting its citizenry. Indeed, "Everybody Wants to Rule the World." Especially the NSA.

So let's suggest ways that the use of the Quiet Enjoyment Infrastructure could refocus government security agencies on protecting people instead of pretending to protect people while doing something else.

Lawful Interception

When is it okay to surreptitiously intrude upon private communication? Government policies are all over the map. At one extreme we have Canada, where complete freedom of encryption has spawned a small industry providing cryptographic products and services that cannot be exported from the United States. At the other extreme we have the United Kingdom, which passed the draconian Regulation of Investigatory Powers (RIP) Bill. RIP gives any police department the right to demand that a private communication be decrypted or a private encryption key be handed over. The legislation clearly breaches human rights standards under the European Convention on Human Rights. American technologists who were aware of the U.K.'s RIP considered themselves fortunate to at least have "freedom of encryption," if not freedom to make and sell cryptographic products. Then the National Security Agency revelations of 2013, particularly the disclosure on September 5, 2013, of NSA's breaking of popular encryption methods, dispelled that fortunate feeling.

The European Telecommunications Standards Institute has been considered a leader in defining appropriate criteria for lawful interception. In ETSI's words,

Lawful interception plays a crucial role in helping law enforcement agencies to combat criminal activity. Lawful Interception of public telecommunications systems in each country is based on national legislation in that country. The purpose of standardization of lawful interception in ETSI is to facilitate the economic realization of lawful interception that complies with the national and international conventions and legislation.

But while ETSI was debating the fine points of lawful interception, the steady stream of revelations in 2013 about the NSA, the U.K.'s GCHQ, France's Directorate-General for External Security, and other effects of the Edward Snowden disclosures revealed that the snoopers aren't really that concerned about thwarting terrorists. *Propublica* noted[73] in September 2013:

> The full extent of the N.S.A.'s decoding capabilities is known only to a limited group of top analysts from the so-called Five Eyes: the N.S.A. and its counterparts in Britain, Canada, Australia and New Zealand. Only they are cleared for the Bullrun program, the successor to one called Manassas — both names of American Civil War battles. A parallel GCHQ counterencryption program is called Edgehill, named for the first battle of the English Civil War of the 17th century.
>
> Unlike some classified information that can be parceled out on a strict "need to know" basis, one document makes clear that with Bullrun, "there will be NO 'need to know.' "

"Making it clear that there will be no need to know" makes it clear that the perpetrators of this crime really want what all despots want. They want power. The possibility of abuse of any lawful interception process is obvious. The ability to designate someone as a suspect constitutes a lot of power, and applied on a global scale, that power can be hugely dangerous.

Apprehension of terrorists is just an excuse. And if the pursuit of terrorists requires yielding our freedoms, the terrorists win anyway.

[73] "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security," by Jeff Larson, ProPublica; Nicole Perlrothand and Scott Shane, *The New York Times*, Sept. 5, 2013, http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

So Let's Just Fix It

Those who lack imagination and insight into the way complex problems are routinely solved fall into the "you can't have security and privacy at the same time" idiocy, as expressed[74] by Slate's Thomas Rid in September, 2013:

> Privacy is fundamental in an open democracy. Without privacy, there is no democracy. Security is also fundamental. Without security, there is no democracy, either. This creates a dilemma: A crucial public good is pitched against a core individual right. No society can maximize both at the same time. The consequence is that we, as a society, have to agree on a compromise,

Everywhere you turn you see systems and devices that optimize two or more features and their benefits in a way that would have seemed impossible had it not actually been done. Just look at your smartphone.

It just takes engineering — by engineers rather than policy wonks or bureaucrats. It takes an effort by those who enjoy applying imagination and discipline to accomplish the impossible — and then enjoy doing it better in version 2.0. Public-minded engineers like Jefferson, Paine, Washington, and Franklin would relish the challenge.

So let's be practical engineers about it. We've learned from centuries of trial and error how effective a system of checks and balances in government can be. Let's keep the emotions aside for a moment and think about how to apply the kinds of checks and balances we have used with branches of national governments.

With the Accountability Component, any authorization of lawful interception, and any actual performance of lawful interception, must be accompanied by an authorization that is digitally signed by the individual officer responsible. The acknowledgement will specify the date that its existence will be subject to public disclosure, with a maximum of 20 years. And so any officer who uses lawful interception will know that there are personal consequences.

Our major concern is to prevent despots from using lawful interception as a means to increase their power and control over people rather than as a tool for legitimate law enforcement. One measure of a country's place on a "totalitarianism scale" is the proportion of suspects to the total population. With Stalin, everyone was suspect.

With the Accountability Component, statistics on lawful interception can be captured using publicly visible algorithms, supervised by boards of knowledgeable citizens, without disclosing any bits of information about the identities of those whose communications are being intercepted.

The portion of the total population that is subject to lawful interception is to be set

[74] "The Rest of the Snowden Files Should Be Destroyed," by Thomas Rid, Slate, September 10, 2013, http://www.slate.com/articles/technology/future_tense/2013/09/nsa_surveillance_the_rest_of_the_snowden_files_should_be_destroyed.html.

by law. Let's say that portion is 1%. Everyone, including the officers, will be aware of the current ratio of suspects to citizens.

If the actual proportion of those being monitored to total population were published monthly and made a matter of public policy, a rising percentage would have to be accompanied by an explanation: war, real civil unrest, etc. A rising suspect ratio would be a sign to the population that the leadership has to resort to surveillance too often and perhaps needs to be replaced. A low or declining suspect ratio is a good sign and a credit to the leadership.

Stalin would not have been able to perpetrate his reign of terror if he were compelled to limit his surveillance to a very specific and small portion of the population. The terror came from the fact that everyone knew that at any moment they and all of their acquaintances could be sent to the gulag.

An Officer's Signature

The initial fear of those who followed the Snowden leaks was that the NSA had made mathematical discoveries that broke AES, RSA, and other encryption/decryption algorithms. Gradually, it became clear that its methods for getting into your encrypted communication are much more mundane than that. According[75] to Bruce Schneier,

> Now that we have enough details about how the NSA eavesdrops on the internet, including today's disclosures of the NSA's deliberate weakening of cryptographic systems, we can finally start to figure out how to protect ourselves…
>
> The NSA deals with any encrypted data it encounters more by subverting the underlying cryptography than by leveraging any secret mathematical breakthroughs. First, there's a lot of bad cryptography out there. If it finds an internet connection protected by MS-CHAP, for example, that's easy to break and recover the key. It exploits poorly chosen user passwords, using the same dictionary attacks hackers use in the unclassified world.
>
> As was revealed today, the NSA also works with security product vendors to ensure that commercial encryption products are broken in secret ways that only it knows about. We know this has happened historically: CryptoAG and Lotus Notes are the most public examples, and there is evidence of a back door in Windows. A few people have told me some recent stories about their experiences, and I plan to write about them soon. Basically, the NSA asks companies to subtly change their products in undetectable ways: making the random number generator less random, leaking the key somehow, adding a common exponent to a public-key exchange protocol, and so on. If the back door is discovered, it's explained away as a mistake. And as we now know, the NSA has enjoyed enormous success from this program…

[75] "NSA Surveillance: A Guide to Staying Secure," by Bruce Schneier, The Guardian, September 6, 2013.

> How do you communicate securely against such an adversary? Snowden said it in an online Q&A soon after he made his first document public: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."…
>
> Snowden's follow-on sentence is equally important: "Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."
>
> Endpoint means the software you're using, the computer you're using it on, and the local network you're using it in. If the NSA can modify the encryption algorithm or drop a Trojan on your computer, all the cryptography in the world doesn't matter at all. If you want to remain secure against the NSA, you need to do your best to ensure that the encryption can operate unimpeded.

Schneier then offers advice on what to do to protect yourself (two of five points):

> Be suspicious of commercial encryption software, especially from large vendors. My guess is that most encryption products from large US companies have NSA-friendly back doors, and many foreign ones probably do as well. It's prudent to assume that foreign products also have foreign-installed backdoors. Closed-source software is easier for the NSA to backdoor than open-source software. Systems relying on master secrets are vulnerable to the NSA, through either legal or more clandestine means.
>
> Try to use public-domain encryption that has to be compatible with other implementations. For example, it's harder for the NSA to backdoor TLS than BitLocker, because any vendor's TLS has to be compatible with every other vendor's TLS, while BitLocker only has to be compatible with itself, giving the NSA a lot more freedom to make changes. And because BitLocker is proprietary, it's far less likely those changes will be discovered. Prefer symmetric cryptography over public-key cryptography. Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can.
>
> Trust the math. Encryption is your friend. Use it well, and do your best to ensure that nothing can compromise it. That's how you can remain secure even in the face of the NSA.

Schneier illustrates one reason among many why all InDoor software is open source. Anyone can pick through the code looking for ugly things such as back doors.

InDoor code is digitally signed by a licensed professional building inspector, that is, a code auditor. Why shouldn't we require that of all code, particularly code that runs the security programs in our computers and phones? If every police patrolman is a public officer, individually applying public authority in the performance of his or her job, why shouldn't the NSA require officers to act as officers and as licensed professionals, digitally signing the code for security products upon which we depend? If the software turns out to be corrupt, we know whom to hold responsible.

Of course is unlikely to do anything of the sort, especially as it appears to view us as an enemy that it won't want to aid and abet.

Key Escrow

Lawful interception is invoked for things other than international terrorism. Detectives also want to use it in the normal investigation of drug dealers, embezzlers, human traffickers, money launderers. Should they be allowed to? If so, then access to keys by law enforcement is necessary.

Key escrow, that is, the maintaining of copies of PKI private keys (PENs) and symmetric encryption keys, is a practical necessity for any system where keys protect anything of importance, because a lost private key means loss of important information. And of course if a key pair didn't protect anything of importance then it wouldn't be used in the first place.

When does the escrowed copy of a private key (or "PEN") go from being a necessary safeguard, kept by the Attestation Officer to replace a lost identity device, to an object of the attention of law enforcement? And who is to say that an individual must have an escrowed private key in the first place? Why shouldn't a person be allowed to take a chance of not being able to recover his or her own information?

Some countries will not allow the use of non-escrowed keys. How does that affect a user communicating with someone in a country that does allow non-escrowed keys?

Recall how the PEN Component works. The Osmio VRD Birth Certificate contains the public key of the "root" key pair that identifies the individual. It will be issued according to the desires of its user and the law of the jurisdiction in which it is issued. If a non-escrowed key pair is issued and used, then we must rely upon the integrity of law enforcement to not automatically suspect its user of doing something illegal. On the other hand, if the user's name pops up in connection with suspicious activity, the fact of the use of a non-escrowed key will be hard to ignore.

In the case of an escrowed key, due process will call for the issuance of a court order for recovery of a private key without notification of its owner.

To see the current state of development of

The Accountability Component

…and to learn how your

experience in international law and law enforcement

might be put to use in its development, please go to
the Accountability Component Development Office at osmio.ch

That wraps up the six components of the Authenticity Infrastructure, that is, the "people" part of the Quiet Enjoyment Infrastructure. Establishing authenticity has involved a lot of bits and pieces, so before we move on to the second major part of QEI let's put together a mnemonic device to help us remember it all.

Where do we want to get? We'll know we have reached Authenticity when we have:
DIgital Signatures Everywhere DISE

But wait. A digital signature is useless unless you know who did the signing, right? Those digital signatures need to come from a certain kind of source, one which is:
Measurably Reliable MER

Those Measurably Reliable sources need to represent individual human beings, in a way that prevents man-in-the-middle attacks, That means
Identity Certificates IC

How do we ensure that the subjects of those identities protect those certificates, and especially their private keys? If they're owned by their users, protecting the users' own personal information, reputations, and assets, they'll be better cared for…
Owned by the User OU

But a credential that's usable everywhere can be a threat to privacy, unless it's part of a properly-designed infrastructure. The solution must preserve and must protect
Privacy P

while also providing Accountability. How will both be accomplished? Through
Accountable Anonymity AA

And so if anyone asks what's so good about the Authenticity Infrastructure just tell them that it's good because it provides DISEMERICOUPAA!

Hey, I didn't say it's a pretty mnemonic.

OK, it's an ugly and not all that memorable mnemonic. But identity solutions are necessarily complex. Making sure they do the job calls for checklists that that help us keep from forgetting important pieces. DISEMERICOUPAA is just a checklist of things that a good identity solution must provide.

Now that we've covered the people part of QEI let's move on to the second of the three major parts of the Quiet Enjoyment Infrastructure, the places part, the InDoors Infrastructure.