U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE AND TECHNOLOGY

Planning for the Future of Cyber Attack Attribution

July 15, 2010

Edward J. Giorgio
President and Co-Founder
Ponte Technologies

1. Answers to Committee Questions

1.1 Is Attack Attribution a Deterrent?

Question 1: As has been stated by many experts, deterrence is a productive way to prevent physical attacks. How can attack attribution play a role in deterring cyber attacks?

Attack attribution is much easier in physical space, but also possible in cyber space. One of our goals is to discover who is attacking us, not whose computer systems they are using to launch their attack, or where geographically those systems are located. However, even this is not enough for a diplomatic or public opinion deterrent. Consider for instance the recent attacks on Google. There is little doubt that these were perpetrated by a state-sponsored actor in China, but has the attendant publicity done anything to reduce the number of cyber attacks coming from China?

Attack attribution is an essential part of our overall situational awareness and emergency response measures. For example, we can use attribution to shut down or otherwise protect ourselves from attacks in progress. We can even stop a DDoS attack without attribution as to the initiator of the attack. We just need to stop where it is coming from. However if attribution is to have any value as a deterrent then it needs to be both irrefutable and able to be revealed to the world without compromising privileged information or intelligence assets. In some cases you can show China was a transit point for an attack and didn't stop it; this has value too.

Current technologies allow us some level of attribution, most of which is plausibly deniable. Attribution can sometimes be made irrefutable by combining what is publicly known with the resources available to an intelligence agency such as NSA or the FBI, but this is rarely releasable beyond government circles – much less to the attacker – and thus has little if any value as a deterrent. There is also the option of turning it into a US State Department demarche to the offending country, but even this has pitfalls (like revealing very sensitive sources and methods).

As with any other form of attack, there are numerous types of organizations or individual involved, and some of these may well be deterred from pursuing a cyber attack for fear of attribution and the legal or economic consequences thereof.

Entities whose systems are used as the launching point for somebody else's attack may also be motivated by attack attribution to secure their systems and either stop an attack in progress or prevent such abuse in the future. It is often possible to identify the reputable private institution who owns the offending computer - if this is made public, it can have an adverse impact on the brand of that institution, revealing ineffective controls and poor information security practices. Corporate executives could be held personally responsible for such failures and personally liable if there is damage to shareholder value.

The same could be true of the ISPs whose networks are used to propagate cyber attacks. Where strong competition is present in the market, attribution can play a valuable role in motivating ISPs to address user education, network monitoring, and endpoint security.

With attacks from nation states, or state-sponsored actors, the potential impact of attribution technologies really depends on the nation, and so our response needs to be carefully tailored to that nation to have maximum effect. Some nations will act cautiously, fearful of the consequences that could come from being exposed as a cyber attacker, such as economic damage, sanctions or even war. Other countries do not seem to care. For those nations that do care but also have a strong offensive cyber presence, masquerading as an organized crime entity, or as a country that is well known to be the source of cyber attacks, is an easy way to reduce such risks.

Terrorist groups will not be deterred by attack attribution - they may even welcome it. However, if attribution can be used as a means of geo-locating members of a terrorist group during an attack, this is something that can be used to disrupt their operational tempo.

For organized crime, attribution may serve as a deterrent if that attribution could be used to help build a criminal case against them that will stand up in court. Unfortunately, their chosen targets may not have the situational awareness to know that they are being attacked, or the resources to provide that deterrent. Organized crime groups will often target either bank customers or small companies with vulnerable credit card databases. When they target the government, they will often target individuals rather than organizations - for example to discredit police officers by planting incriminating evidence on their home computers, or to bribe or blackmail insiders to monitor or affect the course of criminal investigations.

When forensic analysis or other collateral information also permits us to identify the actual human offender, criminal charges, prosecution, and conviction will serve as strong deterrents. This will be somewhat expensive to do here in the US, very complicated with even close allies, and nearly impossible with the bad foreign actors mentioned above. Consider for example the case of Gary McKinnon, who after 8 years is still awaiting extradition from the UK – a very close ally. The legal costs arising from the investigation and long extradition process, along with any future trial, could easily exceed the actual damage of which he is accused. Once a suspect is convicted, their subsequent imprisonment is also expensive. Is this actually a good use of taxpayers' money? We simply do not have the resources to pursue every hacker out there, or even a significant subset of them, much less extradite them to the US and imprison them here.

The last significant group of attackers is the "script kiddies" – typically the easiest attackers to identify, as well as the easiest to protect against. While we should take measures to protect our systems against such attackers, and take measures to identify and deter them where possible, we should keep in mind that many of them really are children. Notwithstanding the damage they cause, our goal should be to guide them towards a more enlightened path in which they become useful and productive members of society, rather than criminalizing them at an early age, which could leave them with no job, no vote, and no stake in the common good.

1.2 Roles of Government & Industry in Technology Development

Question 2: What are the proper roles of both the government and private industry in developing and improving attack attribution capabilities? What R&D is needed to address capability gaps in attack attribution and who should be responsible for completing that R&D?

While company-to-company and nation-to-nation political dialog may well do with less stringent, but plausible, attribution, if attribution is to be used in court then it must be irrefutable and presentable as evidence in its own right. To achieve this, we will have to move to new protocols in the infrastructure which change the very foundation of our networks, building in attribution and accountability from the ground level. Governments and private enterprises are facing similar threats, and trying to solve much the same problems, and so partnerships with industry will help to develop the protocols of the future.

Having built the necessary protocols in collaboration with industry, we can begin to require that entities with a legitimate presence in DoD networks, or in some civil government or critical national infrastructure networks, implement the new protocols as a pre-condition to network access. Some corporate enterprises (particularly in the financial space) will be motivated to do the same for their own business reasons. In this way we can add to the security posture of those networks at the same time as we demonstrate the viability of the enhancements.

This is not something that any one government can push through for broad use in the Internet as a whole. Evidence of this is in the recent claims over the "militarization" of the internet which is not embraced by business, academia, and civil libertarians alike, and even debated within government circles. This is somewhat recognizant of the crypto wars fought two decades ago which ultimately resulted in government conceding the issue. The fact that we may have to make concessions on this issue, should not prevent us from pursuing R&D which will be necessary if/when some politically viable path emerges.

In spite of this resistance to militarization, there are strong economic drivers in global electronic commerce that are pushing towards solving security problems in the infrastructure rather than in the application space. Applications can't sit around waiting to do a time critical task while depending on an unreliable infrastructure. The infrastructure will ultimately enforce stronger authentication for users and terminals, stronger integrity, and non-repudiation assurances for the transactions. These properties, once built into the infrastructure, will serve to decrease gaps in attack attribution capabilities. Infrastructure will always move more slowly than applications, and we should not ignore how quickly application changes can deliver either (and sometimes both) improved privacy and improved attack attribution.

Many credible experts claim the goal, even if deemed reasonable, is not technically feasible. That may be the case to a purist, but the fact that we can't find perfect security solutions anywhere has not deterred us from raising the bar very substantially through many hard fought for improvements.

While government cannot by itself mandate changes in underlying infrastructure technologies (Ex. IPv6), DARPA, NSF, and the research elements supported by the Comprehensive National Cyber Initiative all should be working to research and develop new capabilities. These could be researched, designed, implemented, piloted, and ultimately become operational on DoD and Intelligence networks, where attack attribution is far more important. After all, it was the original ARPANET where current internet protocols were developed and incubated before they ultimately flourished on today's internet.

New protocols based on the above research should be introduced through the IETF, as this process is the most likely to encourage commercial acceptance and deployment into worldwide networks. For security standards or algorithms, NIST is the appropriate agency.

Research in attack attribution would leverage many of the capabilities already developed. We have seen frameworks which securely embed the user ID, computer ID, process ID, institutional affiliation, and geo-location directly into the IP address. One way to do this is with cryptography and allows us to bind the above attributes to the IP address in a non-forgeable way. Continuous improvements in this area could also raise the bar significantly.

We envision transitioning to a multi-protocol internet infrastructure where services offered over DoD network segments would require transmission using these protocols, while other government services such as "Radio Free America" might be offered over network segments which allow or indeed welcome interaction with anonymous entities. Some incremental improvements in this arena are already being made, for example with Trusted Network Connect, which can be used to require machine-level attribution before network access is granted. Similarly, financial institutions might have far more stringent attribution requirements than a news media or marketing agency. Social networking sites would be adaptable to the needs of their constituencies which, I might add, will likely reflect generational differences over the need for privacy.

1.3 Distinguishing Factors between Anonymity and Privacy

Question 3: What are the distinguishing factors between anonymity and privacy? How should we account for both in the development and use of attribution technologies?

Privacy protections are usually given to people who are acting under their true identity while anonymity assumes that people are acting under an anonymous persona. Under privacy, public and private institutions have Personally Identifiable Information (PII) which is bound to other information they retain about their customers. This might be something as simple as the address of a customer who buys firearms. They have policies about protecting such information. Control objectives focused on privacy attempt to mitigate loss from:

a. Unauthorized Individual - Information systems are inadequately protected resulting in a release of data to unauthorized parties inside (or outside) the institution.

b. Authorized Individual - An authorized individual within the institution makes a unilateral decision to overstep their authority and release or sell privacy information.

c. Questionable Institutional Practices - Questionable (and generally accepted) institutional practices push the legal envelope too far by broadly interpreting the privacy laws pertaining to their business.

d. Systemic Institutional Corruption - Systemic institutional corruption results in the willful and unlawful release of privacy information.

In all the above cases, the institution has privacy information which it did not provide adequate protections for. This is not the case with anonymity which would have prevented the institution from knowing the identity of or having PII on the individual in the first place. This is quite different from well intentioned anonymizers which attempt to remove all PII information from data records so they can be used for other purposes, such as research, public health, crime statistics, etc. There have been some failures of anonymized data bases which revealed PII information through “data leakage” or “correlation handles”.

There is very relevant research on the problem of working with Internet router flow records which were anonymized by having random substitutions applied to their IP address fields. Researchers were able to recover the actual IP addresses from a collection of anonymized records and known IP address segments. Since the purpose of attack attribution is to identify the attacker, the attacking computer, or the geo-location of the computer, this cannot be done successfully without unmasking someone or some computer who was attempting to be anonymous. Of course, this is not the case if the person was acting under a “anonymous persona” in the first place, in which case there is no persona to attribute the attack to.

Where true anonymity is allowed, attribution is neither desirable nor possible. Therefore a risk management decision has to be made as to how much anonymity is allowed and in which

contexts. A news organization may consider it more important to allow anonymity to protect journalistic sources, while a DoD organization may see no need for others having anonymity but every need for security. Today's networks give us a mix between anonymity and security, but no fine-grained tools for managing the trade-off between them.

Many of the transactions on the internet are reasonably private but not anonymous. The financial institutions develop protocols which protect the integrity of the financial transactions, and the merchants may make some attempt to protect customer privacy information, but existing protocols don't allow anonymity where it may be called for. For example, I may wish to research AIDS treatments without letting my search agent know that it is me doing this research. I may even want to buy such treatment without revealing my identity to the merchant who is selling it to me, but I may want the supply chain and the public health officials to know what treatments are of interests to this anonymous purchaser. All of this is possible with the right protocols. In the standards section below we will demonstrate the type of research that is needed to develop such protocols.

In order for online commerce to flourish, there is a strong need for trusted entities to issue trustable and non-transferrable identity certificates. In this way people can be assured that when they communicate with the same online identity twice they are actually talking to the same person both times. Governments around the world already issue physical identity certificates, but in the online world governments came late to the game and private organizations such as Verisign have arisen to fill this gap. Any attempt by government to take back control of online identification, or even just to provide services in this space, will be met with resistance.

Leaving aside the issue of who is issuing identity certificates, and how they are secured so as to be non-transferrable, some of these should uniquely identify the holder while others should be able to provide less or even no identity information. It should be possible to acquire as many such identity certificates as are needed, and unless they contain personal information in common between them there should be no way to link one anonymous identity to another. Some organizations already provide physical analogs, in the form of pre-paid credit cards, or pay-as-you-go cell phones, that require little or no personal information to activate.

1.4 Need for Privacy and Attack Attribution Standards

Question 4: Is there a need for standards in the development and implementation of attack attribution technologies? Is there a specific need for privacy standards and if so, what should be the government's role in the development of these standards?

Technologies that are built into the network architecture need to be made in accordance with open standards, as this promotes interoperability and encourages broad adoption. Technologies for attack sensing and mitigation are more difficult to standardize, and standards may actually harm you because they give the attacker something to test their strength against before they come after you.

So, the military will always have to have secret capabilities for attack attribution in addition to the infrastructure standards discussed in the previous answer. These secret capabilities become problematic when the military is asked to apply them to other government agencies, critical infrastructure, ISPs, academia, and international corporations where transparency is vitally important. This is at the heart of the current Einstein debate which is considering the deployment of military intrusion detection capabilities to protect civil agencies. The only solution I see to this problem is a public-private partnership (or standing commission) where technical expert members have government security clearances while not required for other commissioners who, over time, learn to trust in the unclassified explanations given to them by the technical experts.

In the previous answer, we explained the need for standards involving authentication, integrity, confidentiality, non-repudiation, geo-location, institutional affiliation, and more at the infrastructure level which bind all these attributes to the IP address of the end user. We would add an anonymous persona standard as well as new standards to protect privacy. The government should invest in the development of these standards, but let the open standards groups such as IETF, NIST, ISO, WWC, and more run those standards though their respective processes. The government should have representation at the table.

There is a specific need for new and improved privacy standards. We can best illustrate this by introducing a suggested framework for two important areas where privacy is critical: medical records and on-line transactions. This framework should make it clear that existing protocols for on-line transactions focus on the integrity of the financial transaction rather than the privacy of the parties involved. The framework appears in the last section.

2. Full Discussion

2.1 Introduction

If we are to protect the Internet and its users from criminals, hostile nation states, and terrorists we will have to both design the Internet better and then be vigilant about monitoring it. The former will encourage technologies such as strong authentication, while the latter will likely force us to balance Security (attribution) & Privacy (anonymity) when designing new Internet protocols and host technologies. This may appear strange because, at some level, Security and Privacy (S&P) have a similar definition: ***The right to live out one's life without interference from others***. Indeed we can demonstrate many instances of best practices in computer & Internet security which result in enhancing both security and privacy simultaneously. The very existence of these synergistic outcomes, however, permits arguments that can be used to deflect the discussion away from other areas (like attack attribution) where we frequently have to make tradeoffs.

We say frequently above because it depends on the nature of the attack. Is it a National Security threat, or a criminal action and thus in the law enforcement domain? Attribution techniques sufficient to identify a Nation State initiator of an attack for appropriate political/military response need not impact personal privacy. If it is a criminal attack against banks or persons, "following the money" may be more effective in gaining forensic-quality evidence for court action, as opposed to machine identities used merely as clues as to where to start the hunt for physical evidence of crime.

Privacy and anonymity currently play a critical role to many of us here in the US and to freedom fighters, whistle blowers, bloggers, and amateur reporters in both democratic and repressive regimes all over the globe. It's one of the few mediums where you can be relatively anonymous. Unfortunately, the trend line looks ominous for those capabilities and I think these traits will largely disappear in the Internet in 20 years independent of the best intentions of some governments. This prediction is a function of where the Net came from and the fact it's grown so fast and that it had to maintain the original assumptions which drove Internet plumbing (protocol and router development) in the first place and were friendly to anonymity interests. That said, the net is maturing, and as new protocols come online and a new generation of users grow up, the inevitable degradation of privacy is already well underway. In spite of the best efforts of civil libertarians, the current privacy issues are largely business driven. That is, you could still be anonymous if you wanted, but once you jump into the social networking or online commerce pool, it goes away quickly. It is highly likely that the next generation of internet protocols will have the capability to provide much stronger levels of attribution which will, as a byproduct, serve the interests of those seeking attack attribution. So our lack of privacy and anonymity in portions of the future internet may be inherent in the infrastructure, as well as a byproduct of the applications that ride on top of it, as is the case today.

Geo-location is perhaps one of the greatest threats to both privacy and anonymity. The trend towards wireless mobility is embedding location tags deep in the infrastructure which will be imposed by the new protocols that are difficult to circumvent. These protocols may also embed attributes such as personal identity, hardware identity, physical location, and institutional affiliation right in the internet protocol address. This trend will be business driven as national and international commerce will benefit from the stronger integrity and non-repudiation assurances for the transactions. Strong authentication of the person at the other end will be available from the infrastructure rather than from some application operating over it.

These capabilities will serve us well in emergencies caused by natural disasters, man-made accidents, or hostile foreign threats; tweeters, bloggers, and social media players will get their news and pictures from someone at ground zero, rather than having to first sort through the political rhetoric emanating from a distant corner of the globe. These capabilities will have many other benefits, such as providing parents with the real time location of their children. They will also be used for nefariously purposes by criminals, rogue nations, industrial competitors, and terrorists. Wouldn't the terrorists like to turn the tables and know when key US public officials or military commanders are dining in a restaurant?

When balancing the need for anonymity with attack attribution, there is no silver bullet, be it technology, policy, economic incentives, or cultural change, which will solve the problem. Even in cases where attack attribution is deemed more important, we don't currently have reliable ways of actually doing it. Furthermore, when we can identify the offending computer with high probability we may not know who the actual human offender is. This is true because the computer owned by the innocent user may have been previously commandeered by a malicious and anonymous adversary operating from a remote location anywhere in the world. For this reason corrective action such as quarantining the offender may actually be depriving the real computer owner of vital and even life supporting services delivered over the internet.

For the reasons stated earlier, it seems reasonable that individuals should have the right to have an "anonymous persona" – or as many of them as they need – which they can use for online interactions. One ought to be able to anonymously check out the prices in Amazon and Borders before making a purchase; one ought to be able to visit the VA STD site before registering for treatment information; one ought to be able to anonymously read about LAPD civil rights violations; one ought to be able to communicate privately and anonymously with others, while still having some assurance that when we talk to the same anonymous ID we are talking to the same person. Many information providers may chose to only release information to properly authenticated and authorized individuals, but what about sites giving guidance to political dissidents, whistle blowers, oppressed groups, freedom fighters, etc.? These sites, of course, want to share this information privately and without any strings.

In a world of insecure computers and botnets (commandeered armies of innocent computers) we will need attack attribution to point us to the offending computer, its owner or institutional affiliation, and its geographic location. But as computers become virtualized we will lose the ability to attribute action to specific computers and as we move to cloud computing we will even lose the ability to geo-locate the computer. This doesn't mean that we can't encode the

user identity, computer ID, process ID, and institutional affiliation into the computer's (IP) address, because with the proper R&D we can move to a next generation of internet protocols which do precisely that.

2.2 Anonymity

As children, many of us watched a program called "The Invisible Man". Let's suppose that technology makes that a reality where one could take a pill and become invisible for the next hour. This technology might profitably be used to observe nature without disturbing it, visit public places without the fear of recognition and unwanted attention, associate with people we don't want to be linked to, etc. This technology is needed just as much by government entities as it is by citizens. Of course, it is also easy to envision how this technology might be used to commit crime, so we could surely expect a response which would, for example, make it illegal to enter a government building in the invisible state. Banks would respond by refusing ATM withdrawals to invisible people. While all of this sounds like an absurd policy debate, it is precisely what is being played out in cyber space today. Invisible actors from all of the threat groups are ever present in our computers, behind our locked doors, not in the jurisdiction of our courts, not in range of our guns, and overhearing both out thoughts and our private conversations.

2.3 Losing Transparency

As Americans we fiercely defend our right to privacy and security, and subsequently create a vision where we achieve both simultaneously. This vision embodies our protection from individuals, corporations, governments, cultural and religious institutions, subversive organizations, and common criminals. Through our human experience with these actors we recognize that we have reason to fear all of them. Our lives are played out in part through acts conducted by "perpetrators" and which have impact on "victims". While these words are pejorative, it is this concept of becoming a victim that drives our passion for achieving privacy and security. The problem with this logic is that the laws and tools which give potential victims privacy and security can also be used by the threat agents to achieve anonymity. The result is a world with very little transparency into what everybody, from criminals to nation states, are actually doing. Even when we can see the consequence of these actions we may never know who the perpetrators are. One might argue that the history of human social development (and even evolution) was driven by transparency of action. While human nature has remained largely unchanged, we have witnessed three transformations brought about by technology that are having a profound impact on human behavior:

- Attributable to anonymous
- Discoverable to forever hidden,
- Understandable to magical

Wherever we lost transparency, whether into governments, corporations, or individuals, bad actors eventually emerged and violated our trust and laws.

2.4 Who Should We Fear

In America we have a somewhat unique tendency to fear violation of our privacy from government above all. This stems from our beliefs and experiences that if we are wronged by an individual or a corporation we have recourse from damages in a court, while government has historically avoided such accountability. But, let us first explore the expanded threat to privacy and be specific about some of the (largely) foreign threats. Are we not concerned about the Chinese stealing our technology to produce less expensive versions, the Russians engaging in financial crimes, the Israelis' stealing our political intentions, the French stealing our competition-sensitive materials, the Nigerians conning our elderly, and so on? These actors are all foreign threats, and they represent official governments, large corporations, terrorists, and common criminals. And yet, to most of us, these actors are all beyond the reach of our American courts. Our security and privacy is threatened by all of them, yet many folks continue to focus primarily on government. I would suggest that more balance is needed in first identifying the real threat and then establishing the appropriate balance between privacy and security.

Finally, I would be remiss to exclude the fact that while many of these threats are foreign, many are domestic, and, in the past, violations of domestic civil liberties were justified by reference to foreign threat. These are very dangerous constitutional grounds we tread and the gravity of the legal and constitutional dimensions cannot be trivialized.

2.5 Conclusions

In conclusion my comments are not focused on promoting what the ideal balance between privacy and security should be, but rather a challenge to those embracing the utopian view that both may be simultaneously within our grasp. We need to put together representatives from both sides of the debate, allow them to frame the issue, and present the differences in a way our policy and law can respond appropriately. While we will continue to insist that private information remain just that, and that anonymous persona will be supported, the existence of a trusted third party such may be the only way to ensure that. So, the debate might eventually come to: can we trust government with the information it needs to protect our security or do we lose our privacy from a myriad of bad actors (the least of which may be government)? In my opinion government has not yet earned this trust and we will require a lot more transparency and oversight before giving that trust.

In summary, the privacy & security debate (and hence the anonymity and attribution debate) focuses us on only one aspect (albeit very important) of the problem and we need several initiatives to correct that. In parallel, we should also be using our status as a superpower to drive behavior by the Chinese on the internet, the French on business-competition practices, the Russians on stamping out financial crime, the Israelis on influencing our political system, and international crime-fighting organizations on establishing deterrents. This will require a US policy with an enlightened international agenda which focuses on using what remaining superpower status we have to drive behavior. This is essential to balancing security and privacy at home while simultaneously promoting a robust ecommerce and human rights agenda globally. Once such behavior is agreed upon our policy must be "trust but verify" and will

require some authorized (and transparent) monitoring of our information and telecommunications systems, while at the same time, embracing really strong mechanisms to protect privacy and anonymity. This monitoring will allow authorized governments to perform attack attribution with cooperation from the private sector. It will also require oversight by a trusted third party and considerable transparency on Main Street.

3. Appendix: New Privacy Standards Framework

We suggest a new framework to evaluate the security of an on-line transaction. We do this only to elaborate on the inadequacies of the current protocols which focus much more on security than privacy. Our transaction involves a buyer (Bob), a search agent (Goliath), a seller (Sam), a trusted identity provider (Ida), a bank (Betsy), manufacturers (Matt and Martha), the blind anonymity provider (Andy), and finally, Bob's roaming service (Robin). Bob wants to purchase specific goods and begins with asking Goliath to provide a list of sellers. Bob then selects a seller Sam and purchases a product using a credit card he was issued by Betsy. Ida provides some real time assurance that Bob and Sam are who they claim to be. Andy facilitates the sharing of some transaction details with manufacturers Matt and Martha who need to restock the shelves. Note that these latter details are not made available to Andy who is "blind" to the information needed by the wholesalers. Robin provides a roaming and/or backup service for Bob's secret credentials (Robin herself is blind to these credentials).

The security complexity of multi-party protocols grows rapidly as the number of parties in the transaction increases. Our problem potentially has eight distinct roles with some of the roles having multiple players within a specific transaction (such as merchants, manufacturers, or identity providers). Different parties talk both directly and indirectly to each other, security assertions are checked and passed along to other parties, and authentication, integrity, authorization, privacy, and non-repudiation are potentially important to each of the relationships.

We are now in a position to form a privacy framework based on the outcome of several assumptions:

1. Bob knows everything about his transactions.
2. Where Bob has shared his personal information with the other parties, he should still (legally) own that information and be able to update or revoke it at a later date.
3. Ida(s) has provided identity assurance to potentially all parties in the transaction.
4. Goliath knows the set of sellers that have the products Sam is interested in, and, may or may not know Bob's identity.
5. Sam has sold a product to Bob, and Sam may know Bob's identity and his bank account number (today's situation), or Sam knows Bob's identity and mailing address only, or Sam doesn't know anything about Bob.
6. Sam may keep a record of the purchase, but the customer data, and the account information may be kept by Bob only, or by both Bob and Sam.

7. Betsy knows that Bob has made a purchase from Sam, has completed the financial transaction, and may or may not know detailed information about the product that was purchased

8. Matt and Martha know somebody's “purchasing interest” or “purchasing profile”, and may or may not know their identity.

9. Andy has facilitated the transfer of some encrypted data from Bob to Matt and Martha, but doesn’t know what it is.

10. Robin has encrypted information about Bob, including his secret keys, so she can support his roaming, but knows little more than Bob’s identity, and certainly can’t decrypt his secret keys.

The choices in the above framework do not have one-size-fits-all answers, so the ultimate protocol selected must be tunable to the answers that fit the situation.

For brevity, we will not demonstrate a similar privacy framework for medical purposes, but we will point out that there are even more stakeholders in the communications and data retention aspects of any medical situation, and enumerate those stakeholders. They include patient, attending physician, treatment facility, pharmaceutical provider, nurses and other medical care professionals, consulting physician, insurance provider, public health officials, pharmaceutical and infectious disease research community, accounting and billing support staff, and several others. While there are currently many places where anonymizers are used today to share medical information, we believe those protections are woefully inadequate.

4. Ed Giorgio Biography

Ed Giorgio is the co-founder and president of Ponte Technologies, a security and technology company. He is on numerous advisory boards, including the NSA Advisory Board and the Commission to advise the 44th president. He was formerly a principal at Booz Allen Hamilton, where he spent 10 years working on information security and enterprise resilience issues for a variety of commercial clients and federal agencies. Mr. Giorgio also has nearly 30 years of security experience with the National Security Agency (NSA). While at NSA, he pioneered developments in communications security, national intelligence policy and technology, and public key cryptography. Mr. Giorgio is the only person to have served as both Chief U.S. codemaker and, subsequently, as Chief U.S. codebreaker at NSA where he directly managed 1600 mathematicians and computer scientists. As a mathematician, he designed and delivered the first public key based e-mail privacy and authentication system on the worldwide intelligence network. Today he provides services which help clients bridge business innovation, technology, and security and delivers these services to government and commercial clients. He also advises investment bankers and VC's on the viability of early-stage security companies. Mr. Giorgio is considered a leading authority on cryptology and has extensive experience in cryptography, Internet security technology, wireless security, security policy, information warfare, privacy, and intelligence sources and methods.

5. Acknowledgements

I would like to acknowledge the contributions by several people who made critical comments and constructive ideas during the drafting of this testimony. All the views expressed in the preceding text certainly do not represent the positions of the names listed below. Indeed, in some areas, their views represent alternate positions. Never-the-less, their contributions were invaluable.

William Crowell, Consultant, former CEO Cylink, former Deputy Director NSA
Jerry Dickson, former Director of the National Cyber Security Division (NCSD) at DHS
Kevin R. Fall, PhD
Daniel E. Geer, Jr., Sc.D., CISO, In-Q-Tel
Susan Landau, 2010-2011 Radcliffe Fellow, Harvard
Ronald D. Lee, Attorney
James Lewis, Center for Strategic and International Studies
Mike McConnell, Booz Allen Hamilton, former DNI, former Director NSA
Vin McLellan, Consultant and Publicist in Security & Cryptography
Alan Paller, Director of Research, SANS institute
Bruce Potter, CTO of Ponte Technologies, SHMOO founder
Marcus Ranum, CSO of Tenable Network Security
Brian Snow, Cryptographer and former NSA Senior

Finally, this testimony would not have been possible without the content and editing contributions from Patrick Henry of Ponte Technologies.