Lawful Intercept and Advanced Networking Environments

ESCC/Internet2 Joint Techs Workshop

Wednesday, July 18th, 2007 9:30-9:50 AM

Joe St Sauver, Ph.D. (joe@oregon.uoregon.edu)

Internet2 and the University of Oregon

http://www.uoregon.edu/~joe/joint-techs-batavia/

Disclaimer: All opinions expressed in this talk are strictly my own, and do not necessarily represent the opinions of any other entity. This talk is provided in a detailed written form to insure accessibility, and for ease of web indexing. A version of this talk was previously given at Terena TNC2007 in Denmark.

Today's Talk

- I'm neither a lawyer nor a law enforcement person, so this talk is not meant to be legal advice, nor does it in any way express any sort of "official" opinion about CALEA.
- What I've done is to:
  -- look at what law enforcement (LE) appears to want/need,
  -- look at the sort of networks and systems architectures that higher education currently has planned or deployed, and
  -- review some public documents relating to lawful intercept.
- Considering those requirements, facilities and documents, I've then endeavored to discuss and explain the issues which I believe may ultimately frustrate law enforcement's goals and objectives, frustrations which may (and probably should) end up driving requests by them for clarifying amendments to CALEA, and specific technical assistance.

What *Is* CALEA?

- CALEA is the United State's "Communication Assistance for Law Enforcement Act of 1994," see 47 USC 1001-1021.
- Quoting http://www.askcalea.net/, CALEA “defines the existing statutory obligation of telecommunications carriers to **assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization**. The objective of CALEA implementation is to preserve law enforcement's ability to conduct lawfully-authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness.” Recent FCC administrative actions (and court decisions targeting those actions), have clarified that this 1994 law includes “facilities based broadband providers,” and under some circumstances, **some higher education institutions and networks**.

Wiretaps Without CALEA

- Traditionally, wiretapping has been a manual process:
  -- A court of competent jurisdiction would issue suitable an order authorizing a wiretap to occur,
  -- The local provider (whether that's a telephone company, Internet service provider, or other entity) would be contacted by LE and asked to provide assistance
  -- Legal review of LE's request for assistance would occur
  -- Assuming that local legal review is positive, technical steps would be taken to facilitate the requested intercept, such as mirroring a switch port or installing an optical splitter
  -- Traffic from that intercept would be minimized to insure that only traffic covered by the paperwork would be extracted
  -- The minimized traffic would be delivered to LE
  -- LE analysis of the intercepted traffic would then occur
- **This is not a painless, rapid, or inexpensive process.**

Traditional Wiretaps Can't Be Provisioned At "Internet Speed"

- Traditional wiretaps aren't very agile – they don't (and can't!) be provisioned at "Internet speed."
- By this I mean that in many cases a network connection may be used for just a very brief period of time, but traditional wiretaps might take days (or weeks!) to request, approve and arrange, and by that time, the subject of the interception order might be long gone, having moved on through a series of one or more other connections in the intervening time.
- In some cases it may be possible to obtain a court order authorizing a so-called "roving" or "multipoint" wiretap (but those have traditionally been uncommon – only 15 were approved in 2006), and even then, the physical mechanics of effecting the interception can be thwart the intent of the order.
- CALEA may have been designed to partially begin fixing this.

CALEA Wasn't (and Isn't) Perfect

- **CALEA involves many federal agencies**: the lead agencies are the FCC and the FBI, but the DEA and other agencies may also be providing input and direction (and ironically the consensus result may be fully satisfactory to none of them).
- CALEA's evolution and extension to the Internet occurred by the FCC's **creative interpretation of an existing statute**, rather than clear and unambiguous legislative action *de novo*.
- Not surprisingly, CALEA has been the **subject of litigation**, including litigation which yielded a complex and tortured judicial decision which, when read, does little to shore up CALEA's legitimacy as applied to Internet technologies.
- CALEA has had a very **slow roll out**, in part because CALEA involves complex technical matters and required industry help in developing **appropriate technical standards**
- CALEA is also potentially very **expensive**.

CALEA and the DOJ Inspector General

- "According to the Federal, state, and local law enforcement officials we interviewed and surveyed, their agencies do not request intercepts requiring CALEA features for several reasons (i.e., the **high cost charged by carriers**, [...], or the investigation **only required a traditional wiretap**)."
- 'Law enforcement's biggest complaint regarding CALEA is the relatively high fees charged by carriers to conduct electronic surveillance. **A traditional wiretap costs law enforcement approximately $250.** However, **a wiretap with CALEA features costs law enforcement approximately $2,200** according to law enforcement officials and carrier representatives we interviewed. A law enforcement official noted that, “[w]ith CALEA, the carriers do less work but it costs approximately 10 times as much to do a CALEA-compliant tap" [emphasis added]

Additional DOJ Inspector General CALEA Report Comments...

- 'According to the FBI, Internet “hotspots” such as **cyber cafés that provide anonymity with multiple access points**, third-party calls using calling cards, and toll free numbers are a “technologically unsolvable problem.” These services can only be addressed through investigative techniques, rather than through the application of CALEA. In addition, FBI officials said that commercially available electronic **encryption** will also hinder law enforcement’s ability to collect information from electronic intercepts.'
- Lots more interesting data is in "The Implementation of the Communications Assistance for Law Enforcement Act," U.S. **Department of Justice Audit Report 06-13**, March 2006, Office of the Inspector General Audit Division; see http://www.usdoj.gov/oig/reports/FBI/a0613/final.pdf [emphasis added]

Lawful Intercepts by the Numbers

Nationwide, in 2006 (the most recent reporting year available):

- Intercepts authorized by federal & state courts in '06: 1,839 (461 by federal judges and 1,378 by state judges)
- State courts with the most approved intercepts: CA (430), NY (377), NJ (189), FL (98) – those four states accounted for 79% of all state intercept orders; 27 state courts reported no intercepts whatsoever.
- Average days installed wiretaps were in operation: 40 days
- Average number of people whose communications were intercepted per wiretap order: 122
- **80% of all wiretaps involved drug offenses**; racketeering and homicide/assault were the other two top offenses cited.
- Average cost of a federal intercept: $67,044. Average cost of a state intercept: $46,687. [no, I can't explain the difference between those costs and the costs mentioned on slide 7…]

Lawful Intercepts by the Numbers (cont.)

- **Wiretap requests which were for telephones: 96%**
- **Wiretap requests involving mobile devices, such as cell phones: 92%**
- **Number of federal or state intercepts encountering encryption: 0.**
- **Wiretap requests which were for "digital pagers, fax, or computers:" roughly 0.7% (13 requests out of 1,839)**
- **Source: U.S. Courts' 2005 Wiretap Report,** http://www.uscourts.gov/wiretap06/contents.html
- **Note:** these numbers do **not** include FISA intercepts and some selected other categories of interceptions.

  FISA and other national security intercepts dwarf criminal intercepts by law enforcement)

Universities and CALEA Compliance

While everyone always wants to obey the law, many universities (and many academic networks) have determined that one or more CALEA exemptions apply to their situations, and as a result they are NOT making expenditures and establishing procedures to CALEA-enable their networks

The Private Network Exemption

- 47 U.S.C. 1002 (b)(2)(B) exempts "equipment, facilities, or services that support the transport or switching of communications for private networks."
- Unfortunately, "private network" is not explicitly defined in the Act, and it can sometimes be difficult to ascertain exactly where a "private network" ends and "the Internet" begins.
- Clearly, a network which exists solely within a single building or facility and which does not interconnect with any networks owned or operated by other entities would be a "private network" for the purposes of CALEA.
- That sort of physically isolated private network is rare, however, and restricting it to just that one extreme type of "private network" would be unduly and unnecessarily limiting since the **FCC has made it clear that the private network exemption potentially encompasses far more**.

Footnote 100 of the FCC's "First Report and Order and Further Notice of Proposed Rulemaking," FCC 05-153...

"Relatedly, some commenters describe their provision of broadband Internet access to specific members or constituents of their respective organizations to provide access to private education, library and research networks, such as **Internet2's Abilene Network, NyserNet, and the Pacific Northwest gigaPoP**. See, e.g., EDUCAUSE Comments at 22-25. To the extent that EDUCAUSE members (or similar organizations) are engaged in the provision of facilities-based private broadband networks or intranets that enable members to communicate with one another and/or retrieve information from shared data libraries not available to the general public, these networks appear to be private networks for purposes of CALEA.

"Indeed, **DOJ states that the three networks specifically discussed by EDUCAUSE qualify as private networks under CALEA's section 103(b)(2)(B).** DOJ Reply at 19. We therefore make clear that **providers of these networks are not included as "telecommunications carriers" under the SRP with respect to these networks**. To the extent, however, that these private networks are interconnected with a public network, either the PSTN or the Internet, providers of the facilities that support the connection of the private network to a public network are subject to CALEA under the SRP."

Internet Gateway Compliance (Only)

- At one point there was concern that universities would need to replace virtually all their network equipment in order to make it possible to do lawful CALEA interceptions within private networks themselves.
- That is, if you wanted to be able to lawfully intercept traffic going from one local user to another local user, with both users connecting via the private network, it would not be sufficient to just be able to intercept traffic at the Internet gateway -- traffic exchanged between two local users would remain entirely within the local private network, and since it would never touch the Internet gateway, it would not be able to be lawfully intercepted.
- In its second report and order, however, the FCC clarified that in fact private networks did in fact **only** need to be CALEA compliant at their **Internet gateway**.

Internet Gateway Compliance (2)

- See, for example, the FCC's Second Report and Order and Memorandum Opinion and Order, Adopted May 3, 2006, FCC 06-56 at page 82, which states,

  "*Petitioners' professed fear that a private network would become subject to CALEA "throughout [the] entire private network" if the establishment creating the network provided its own connection between that network and the Internet is unfounded. The [First Report and Order] states that only the connection point between the private and public networks is subject to CALEA. This is true whether that connection point is provided by a commercial Internet access provider or by the private network operator itself."*

Then There's Also the Interconnecting Telecommunications Carriers Exemption

- 47 U.S.C. 1002 (b)(2)(B) also exempts "equipment, facilities, or services that support the transport or switching of communications [...] for the sole purpose of interconnecting telecommunications carriers."

- Thus, "equipment, facilities, or services that support the transport or switching of communications [...] for the sole purpose of interconnecting telecommunication carriers" would not be subject to CALEA.

Last Mile Focus

- CALEA's emphasis is thus on so-called "last mile" connectivity, not backbone interconnections between carriers. Why is law enforcement **not** particularly interested in connections between backbone carriers for CALEA compliance purposes?
- Backbone carriers may lack the knowledge needed to identify network traffic that may be associated with a named lawful intercept subject of interest ("All network traffic originated by or destined for Susan Marie Anderson of 345 Elm Street, Wagonwheel, Oregon.") – the backbone carrier would simply have no idea what traffic is associated with that person of interest. E.G., only the last mile provider might know what IP address or MAC address she's using.
- But is the last mile provider **ALSO** CALEA-exempt? Consider the so-called "coffee shop" exemption...

Retail Establishment Exemption

- A final potentially relevant exemption can be found in the so-called **"coffee shop" exemption or "retail establishment exemption"** described at paragraph 36 and footnote 99 on PDF page 19 of 59 of the First Report and Order, FCC 05-153 which states,
"*Finally, in finding CALEA's SRP to cover facilities-based providers of broadband Internet access service, we conclude that* ***establishments that acquire broadband Internet access service from a facilities based provider to enable their patrons or customers to access the Internet from their respective establishments are not considered facilities-based broadband Internet access service providers subject to CALEA*** *under the SRP. [footnote 99] We note, however, that the provider of underlying facilities to such an establishment would be subject to CALEA, as discussed above."* [emphasis added]

Footnote 99

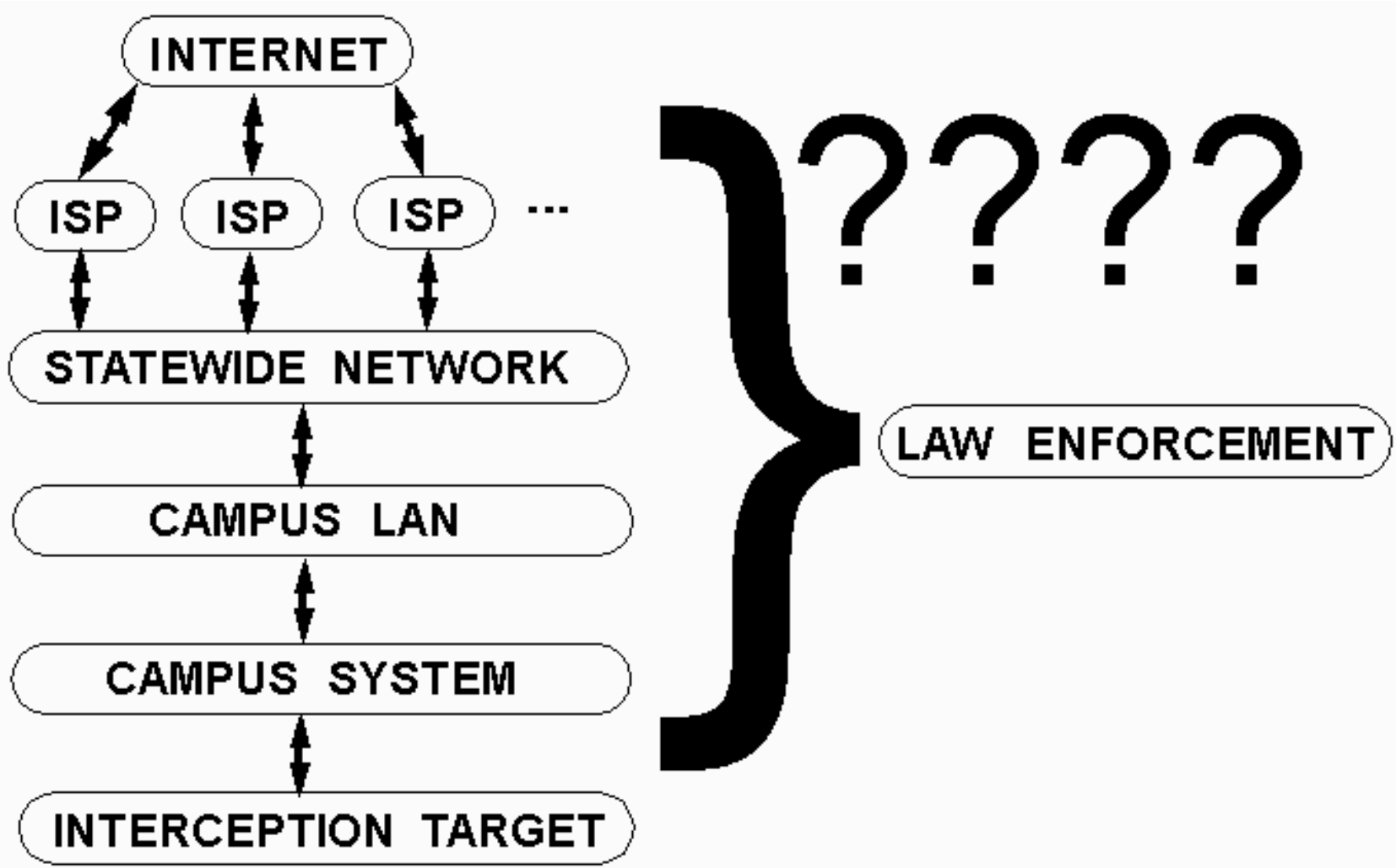
- Footnote 99 reads:

  '***Examples of these types of establishments may include*** *some hotels, coffee shops,* ***schools, libraries****, or book stores. DOJ has stated that it has "no desire to require such retail establishments to implement CALEA solutions," DOJ Comments at 36, and we conclude that the public interest at this time does not weigh in favor of subjecting such establishments to CALEA.'* [emphasis added]

- This exemption might provide additional grounds for some schools to assert that they are exempt from CALEA compliance obligations. Note, too, that it may effectively deprecates the possibility of a hierarchy of exempt private networks, since the "provider of underlying facilities to such an establishment would be subject to CALEA" apparently as an absolute matter by this finding.

One or More of Those Exemptions May Apply to Many HE Institutions

- Because one or more of those exemptions may apply to many higher education institutions, many colleges and universities (and statewide or region-wide higher education networks) have not filed either the “CALEA Monitoring Report for Broadband and VoIP Services” reports, nor a “System Security and Integrity” (“SSI”) Plan, nor have they instrumented their network to be able to deliver CALEA-related data to law enforcement...
- **The net result is that there's tremendous confusion about who must be ready under CALEA to get lawfully intercepted communications to law enforcement...**


INTERNET
ISP
ISP
ISP
...
STATEWIDE NETWORK
CAMPUS LAN
CAMPUS SYSTEM
INTERCEPTION TARGET
????
LAW ENFORCEMENT

Everyone; No One; No One Knows

- Because of the complexities we've been discussing, there's a distinct possibility that **"everyone; no one; no one knows" may be the phrase that best describes who's responsible for being able to lawfully intercept traffic in a complex university network environment.**
- The campus, the statewide network, AND the upstream ISPs may ALL instrument their networks so as to be able to support CALEA, a permissible situation, but potentially expensive "overkill."
- On the other hand, a campus might expect the statewide network to take on that obligation; the statewide network might expect the campuses or the statewide network's upstream ISPs to handle it; the upstream ISPs might expect the campuses or the downstream statewide network to handle it. Ultimately **no one** may be ready/able to respond.

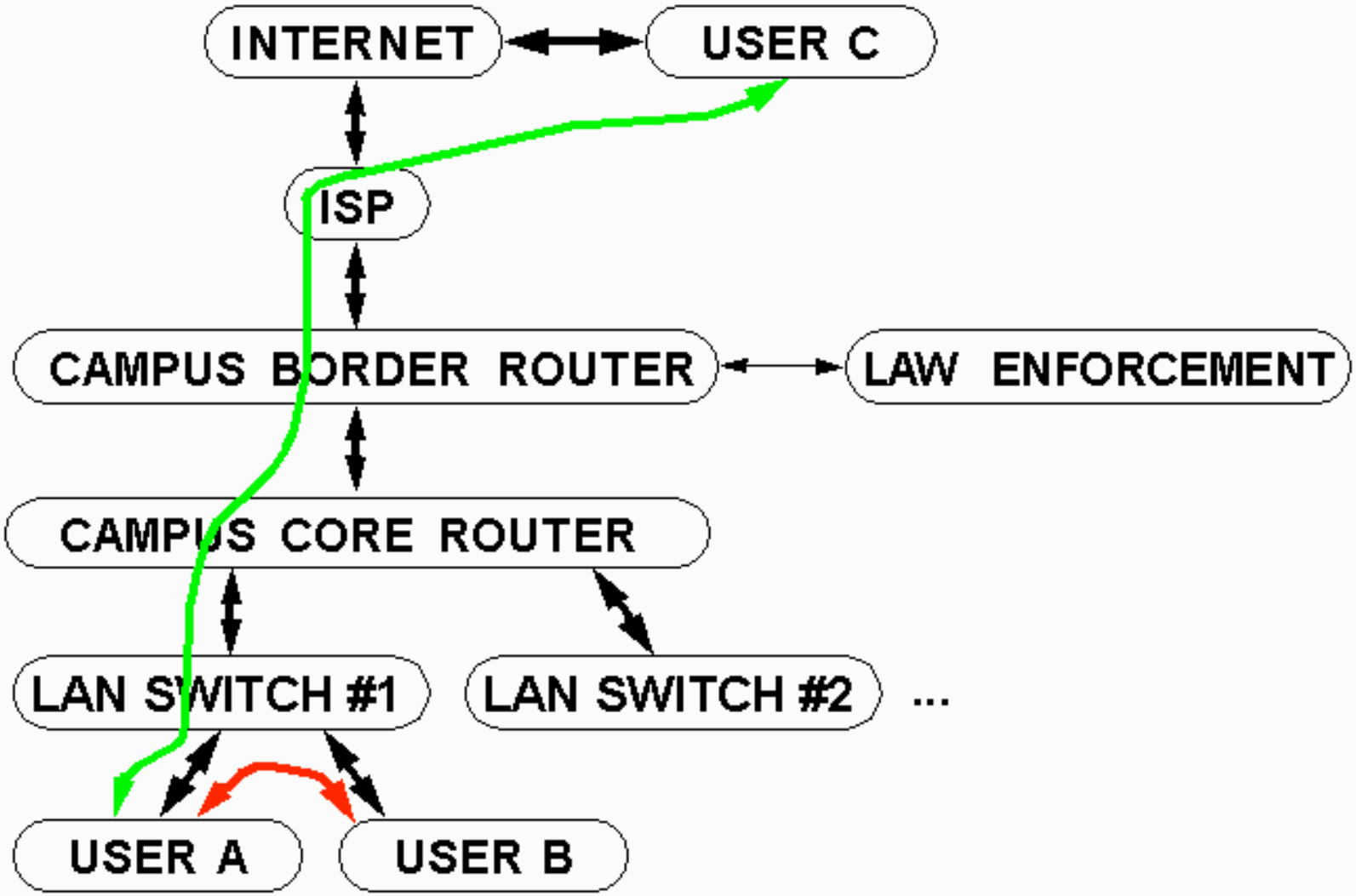
The Costs and Benefits of Doing Lawful Intercept (LI) "Upstream"

- Let's assume for the sake of argument that the connections between the statewide network and a national service provider end up being determined to be the "Internet Gateway," and thus must be compliant.
- Technically, it can be hard to do LI on high bandwidth pipes.
- Remember, too, that the state network may have no idea who's traffic they're delivering by the time it gets to the gateway between the state network and the ISP.
- Finally, at least in some cases, there may be literally millions of users "downstream" from that state network's Internet gateway, and **any** traffic within that network – as long as it **stays** within that "private" network – would not need to be able to be monitored under CALEA's Internet "gateway compliance only" provision.

Even Being Gateway Compliant at the Campus Level May Mean Missed Flows

- Even if we tighten up, and move the compliance point from the statewide network/ISP demarc to the statewide network/ campus demarc, you'll still end up missing internal flows...
- See the red arc on the diagram on the following slide... only traffic that goes through the "Internet Gateway" (in this case shown as the campus border router) would be potentially able to be intercepted.
- The probability that traffic will end up passing through the Internet Gateway is partially a function of how "far upstream" the "Internet Gateway" may be – the more users who are downstream, in the "private network" region below the Internet Gateway, the greater the chance that their traffic will remain local (going to another local user of the private network), and hence be effectively unmonitorable.

Per Port vs. Gateway Compliance: Local Flows Between A&B Don't Touch The Border Router And Hence Aren't Subject to Lawful Interception



Peering at Internet Exchange Points

- Many universities participate in **peering** connections at Internet exchange points (see the list of known public Internet exchange points at http://www.ep.net/ep-main.html).
- Unlike commodity Internet transit connections, or high performance research and education network connections, peering takes place when two networks agree that it is mutually beneficial to exchange customer traffic, and only customer traffic, directly.
- Thus, if two sites exchange traffic via a peering point, traffic between those sites would be:
  -- exchanged directly, and so would not touch "the public Internet" via a commodity Internet transit provider, BUT
  -- I suspect that LE would still expect that traffic to be able to be lawfully intercepted... but wouldn't this would be an "interconnecting carrier"-ish CALEA-exempt situation?

So Where Does "The Internet" Begin?

- So where does the Internet begin? Because the Internet is "just" an interconnected "network of networks," maybe:
  -- the point where I begin to **pay** someone else to carry my traffic (but note that peering points would fail that test!)
  -- the point where **administrative control** shifts from one entity to another (this might even be at a link between a departmental LAN and the campus backbone, on campus)
  -- the point where traffic from one **network address block** leaves that address block and enters a link whose other end has an address controlled by another entity
  -- the point at which the **autonomous system number** associated with traffic changes from one entity to another (but some ASNs, like AS701, represent phenomenally large aggregations of disparate customers!)
- The law should be amended to clarify this key point.

Overcollection and Minimization

Maintaining the privacy of those not covered by a lawful interception order may be hard in many common situations

CALEA: What Was Ordered, And ONLY What Was Ordered

- Another important provision of CALEA is that it requires delivery of what was approved for interception, and **ONLY** what was approved for interception.
- For example, a court may issue an order for either **"pen-register/trap-and-trace"** data or for **"full communication contents"** (what's often referred to as a "Title III" order). The geek way to think about the difference between the two is to think about the difference between doing Netflow, and doing a full packet capture.
- If the court orders the production of **just** flow level data, you **cannot** be lazy and give LE full packet captures instead (if you tried to do so, LE should and hopefully *will* refuse to accept it). You must provide **only** what was ordered.

Minimization

- Another example: if you receive an order specifying the interception of traffic associated with a particular IP address, you cannot respond to that order by simply providing a copy of everyone's traffic – you must minimize what's delivered to be **ONLY** the traffic for the entity specified in the order.
- ATIS-1000013.2007 says a **subject** may be identified by:
  -- their IP address (or set of IP addresses)
  -- an account session ID assigned to the subject at login
  In others cases, the interception order may specify particular **equipment**, rather than a particular person, via:
  -- a MAC address
  -- an IP address (or set of IP addresses)
  -- a circuit ID or ATM or Frame Relay PVC
- Sometimes it may be hard to suitably minimize traffic, and avoid overcollection using those identifiers. For example...

Firewalls with NAT

- Hardware firewalls are a common feature in many network architectures, and are intended to shelter interior devices from external scans and from attack traffic.
- Some hardware firewalls, in addition to deflecting unwanted external traffic, also do network address translation ("NAT"). Linksys Cable/DSL "routers" are one example of a popular consumer hardware "firewall" device which does NAT.
- When doing NAT, all traffic from a NAT box can be made to share a single public IP address, making it extremely difficult to determine if a publicly observable flow is coming from user A, user B, user C or ...
- Attempting to attribute traffic to a particular user typically requires access to the NAT box's log files (which may not even exist, particularly in consumer environments), accurate time stamps, and the cooperation of the NAT administrator.

Some NAT'ing Firewalls Aren't Sitting In Front of "Just a Few" Folks

- Over time, particularly as worries about breaches involving personally identifiable information have increased, there's been a growing tendency at some universities to NAT entire campuses, potentially putting thousands of individuals behind one (or just a handful) of IP addresses.
- While one might think that this strategy enhances the security of the campus ("Hey! Everything's behind a firewall, we must be safe(r), right?"), a campus-wide NAT actually creates a sort of fate-sharing. All users inherit the reputation of the worst user working from behind the NAT device, and a court order asking for "all network traffic" associated with a single public IP address (which could be the public IP address of the NAT box) might potentially include traffic associated with **thousands** of users.

Post-Hoc Minimization

- When there's absolutely no way to minimize intercepted traffic in advance, it may be possible for post-hoc minimization to be done.
- Presumably that could be done for NAT'd traffic just as post-hoc minimization is used to deal with other tricky mixed traffic scenarios, but the process of teasing out one user's NAT'd traffic from the traffic of thousands of other users would potentially be quite daunting, and if done improperly, could jeopardize the privacy of a large number of innocent users who are also behind that NAT.

Dynamic Addressing and Timestamps

- Another complication is dynamic addressing. In general, when a desktop or laptop system connects to a university network, it uses DHCP (dynamic host configuration protocol) to get an IP address, to learn its broadcast address/ netmask/default route, the right name servers to use, etc.
- When dealing with dynamic addresses, as when dealing with traffic that's flowed through a NAT, having accurate time stamps (with time zone information!) can be absolutely key to correctly identifying a party of interest.
- Things can get very complicated if time synchronization is poor, connect times are brief, and IP utilization is high with little idle time between sessions.
- Sometimes users of dynamic addresses authenticate, which can be a big help, but other times users of dynamic addresses may not do so.

Dynamic Addresses Without Auth

- While authentication will usually be required for hosts connecting via dialup, or for hosts connecting via wireless, hosts connecting via a hardwired 10/100/1000 Mbps ethernet connection often do NOT require authentication.
- The rationale behind not requiring authentication for all dynamic addresses is that we know where a given ethernet jack is physically located, so given a known physical location we should usually be able to identify the user.
- The assumption that if we know a jack's location ==> we know who's using that jack breaks down when:
  -- it is applied to shared public spaces, such as classrooms, where anyone can plug a system in without auth
  -- per-port documentation is wrong/out-of-date/non-existent
  -- wiring closets or cabling runs are insecure, etc

CALEA and Advanced Protocols

Higher Education R&E Networks Differ in Material Ways From the Commodity Internet

CALEA Is NOT Supposed to Discourage Advanced Protocols

- 47 USC 1002(b) makes it clear that

  "This subchapter does not authorize any law enforcement agency or officer
  [...]
  (B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services."

- Everyone recognizes that Internet innovation is critical to remaining competitive, BUT does anyone have an out-of-the-box CALEA interception capability which includes handling IP multicast, IPv6, jumbo frames, Shibboleth/ InCommon-based authentication, or extreme data rates?

1) IP Multicast

- Normally, a network session is "unicast" between one source and one destination. For example, you might request a streaming video broadcast from a news web site, and that web site would deliver that video on demand from their server to your workstation. If another person wanted to see that same video, the news web site would then create a second independent video stream, iterating for each viewer interested in a particular video.
- IP multicast is an alternative approach which allows a server to distribute a **shared** network stream which can serve one user, or a dozen, or a thousand, or a million. Because IP multicast is so efficient, a content originator (like an online news site) can afford to distribute TV quality video (MPEG1) instead of postage-stamp-sized herky-jerky video.
- For a technical overview of multicast, see www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/mcst_sol/mcst_ovr.pdf

IP Multicast and CALEA

- Why mention IP multicast today? Well, IP multicast is rare in the commercial ISP space but **quite common** among Internet2-connected universities and I don't think anyone has given much thought to how IP multicast traffic would be handled under CALEA. Relevant issues might include:
  -- IP multicast content is typically delivered via a network tree which gets built to a local router (rather than directly to the interested party), so it may be hard for gateway-based lawful intercept software to recognize that particular IP multicast content is associated with a user of interest
  -- multiple participants (some who may be the subject of an interception order, and others who may **not** be the subject of an interception order) may be accessing or contributing content to the same IP multicast group – what can/should/needs to be done then to protect 3rd party users' privacy?

2) IPv6: Hey, It's Real Too, Folks!

- Most network traffic on the Internet today uses IPv4, but it is projected that within 4 to 5 years we will exhaust available IPv4 address space (see: http://bgp.potaroo.net/ipv4/)
- IPv6 modifies the traditional IPv4 packet format in numerous ways, the most important of which is that with IPv6 network addresses go from 32 bits to 128 bits, thereby dramatically increasing the number of addresses available for allocation.
- Numerous operating systems are IPv6 aware today, including Microsoft Windows Vista, Apple Mac OS X, Linux, Solaris and others. Numerous networks carry native IPv6 traffic in the United States and overseas, including higher education research and education networks such as Internet2, and all .gov core networks must be ready to pass IPv6 traffic by 6/08 (www.cio.gov/documents/IPv6_Transition_Guidance.doc).

ATIS-1000013.2007 and IPv6

- Checking ATIS-1000013.2007, "Lawfully Authorized Electronic Surveillance (LAES) For Internet Access and Services," issued April 2nd, 2007, the string "IPv6" appears 6 times in 75 pages, with the only substantive reference appearing on PDF page 16 where it is mentioned that "The Subject Domain, Access Network, Intermediate Network and ISP Network may be using IPv4, IPv6, or any combination of IPv4 and IPv6 involving translation or tunneling."
- That implies an ATIS-1000013.2007-compliant CALEA implementation should be able to deal with (for example), both native IPv6 frames, and IPv6 traffic tunneled via protocols such as Teredo (see http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx).
- Looking at the marketplace, I'm not seeing commercial CALEA product which fully supports IPv6 intercepts, nor am I seeing IPv6 support in OpenCALEA as of v0.5.

3) Jumbo Frames

- Normal ethernet frames are 1500 bytes long, but that's far too short for optimum performance on long distance, high bandwidth networks characteristic of advanced networks in higher education. Currently both Internet2 and the Federal Joint Engineering Team (JET) recommend use of a 9K MTU:

  www.nitrd.gov/subcommittee/lsn/jet/9000_mtu_statement.pdf

  noc.net.internet2.edu/i2network/documentation/policy-statements/rrsum-almes-mtu.html

- Will CALEA interception devices and CALEA delivery links be engineered to accommodate jumbo frames? Lawful interception gear may or may not be prepared to even **see/intercept** 9K (or larger!) frames, and simple delivery of 9K MTU traffic may also pose issues.

ATIS-1000013.2007 and MTU Issues

- ATIS-1000013.2007 addresses fragmentation in Appendix D.4 "IC-APDU Fragmentation and Optimization (Informative)" (which is not officially part of the standard)
- Because jumbo frames are frequently associated with high throughput connections, practical issues associated with the fragmentation of high bandwidth jumbo frame traffic may be non-trivial to resolve.
- Heck, given encapsulation overhead, even transferring 1500 byte packets will require fragmentation and reassembly.
- It would be great if a normative (rather than just informative) statement on the fragmentation and delivery of jumbo frames could be made part of a future version of this standard.

4) Federated Authentication

- We're all awash in site specific usernames & passwords, so if you trust my school (or other institution), why not agree to:
  -- let them authenticate me via a username & password,
  -- let them share (just) relevant attributes about me with you
  -- then, as may be appropriate, give me access to resources
  See, for example: http://shibboleth.internet2.edu/ and http://www.incommonfederation.org/
- Some examples of federated authentication:
  -- access to a proprietary online database (may be limited by contract to just faculty in a particular department)
  -- access to the now-legal Napster music service (perhaps limited to just undergraduate students at a university)
  -- wireless access to the Internet while visiting another site
- It is the last type of case, which is tricky for CALEA – you may know *what* I am (e.g., I'm a faculty member from Alpha University), but not have any idea *who* I am.

Isn't Shib-Mediated Auth Just An Example of a CALEA Access Network?

- No. ATIS 1000013.2007 describes an Internet Access and Service Model which includes "Access Networks" potentially performing a registration function, REG-F, and a resource function, RES-F, e.g., see figure 1 in that spec. The Packet Transfer Function (PT-F), however always takes place via the ISP network. That model runs into trouble when **authentication** occurs via one's "home institution" but **network traffic** only flows via the facilities of the institution which someone happens to be visiting.
- Yes, retrospectively the home institution could identify a person using the network at the visiting institution, but at that point the identification would be retrospective, and too late -- a party subject to a LI order might have had access to the Internet without his or her traffic being ID's & monitored.

5) Extreme Data Rates

- Unlike dialup/POTS/cell links, broadband connections are (by definition) associated with higher than normal data rates. Typical **consumer** broadband connections might range from ISDN speeds of ~128Kbps to 15-20 Mbps (for things like cable modem connections and fiber-to-the-home services).
- In the case of **higher education**, however, it is routine to see **far** faster connections, including:
  -- 100/1000Mbps on the local area network and
  -- speeds up to 10Gbps to Internet2 or to the regular Internet
- Because these speeds exceed the speeds which are commonly/affordably available to LE via the commodity Internet, there exists the possibility that a subject connecting via a high speed connection may be able to generate network traffic in excess of what LE can cost effectively transport from a local interception point to an offsite LE wireroom.

Two Excerpts from DOJ Report 06-13

- "During our site visits, many law enforcement officials noted that CALEA addresses what carriers need to provide to law enforcement agencies without addressing how **data is delivered.** For example, CALEA does not address whether carriers can use digital or audio phone lines to deliver the audio portions of intercepts. As a result, the delivery method of intercepted data varies by carrier. Due to the various delivery methods, law enforcement agencies must purchase additional equipment to receive the intercepted data from a carrier. The four delivery methods are **dial-out, VPN, frame relay, and T-1 lines**." [emphasis added]
- Discussion of non-VPN delivery methods may indicate a failure to consider the realities associated with higher education's DS3 (45Mbps), 100Mbps, OC3 (155Mbps), OC12 (622Mbps), gigabit, and 10gigabit-class connections.

Heck, LE Doesn't Want to Even Buy T1's

- "A law enforcement official in California stated that his office was informed by two in-state wireline carriers that they are CALEA-compliant but law enforcement would need to build a T-1 line to each of the carriers' switches. The law enforcement official explained that this concept is unreasonable considering his agency's jurisdiction has about 95 switches from one carrier and about 130 switches from the other. Therefore, it would cost his agency about $292,500 to install T-1 lines to each of the switches. This scenario would not be cost beneficial to his agency because a T-1 line is only used for wireline intercepts, and approximately 70 percent of this agency's wiretaps are performed on wireless phones." [from DOJ Report 06-13]
- $292,500/(130+95)=$1,300/line (e.g., that's just installation); monthly reoccurring costs would add another $575-1,800/line

On-Site/Local Wire Rooms

- One possibility which LE might consider would be the build out of local wire rooms to handle processing of high bandwidth flows without the need to purchase wide area, high-capacity, circuits. Once traffic had been transported to the secure on-site wire room, it could then be summarized or otherwise processed, including potentially being written to portable media for offline transport to analysis resources.
- This strategy begins to break down as the number of high bandwidth sites (and thus the number of local wire rooms required) gets large.
- This approach also assumes either a persistent interest in a particular site (justifying permanent facilities), or perhaps the ability to easily deliver a portable wireroom (conceptually imagine something like a preconfigured semi-trailer-based mobile wire room, which could be driven up and plugged in).

Dynamic Circuits

- Conceptually, LE or a university might also consider using a dynamic circuit to deliver high volume CALEA intercept traffic to a LE-designated location.
- What do I mean by a dynamic circuit? Well, that might be a MPLS VPN or other tunnel running over the institution's existing wide area connection (assuming sufficient unused capacity exists), or the use of emerging dynamic lambda facilities (assuming those facilities are available and not already committed).
- Those sort of strategies might allow intercept traffic to be backhauled to one of a small number of regional analysis centers, thereby eliminating the need for LE to either build out local wire rooms at each high bandwidth site, or the need for LE to purchase and maintain dedicated high bandwidth physical circuits to each site.

Conclusion and Recommendations

CALEA can and should be fixed

CALEA Deserves Statutory Cleanup

- CALEA is showing its age, and trying to make a 1994 law that was aimed at traditional telephone services fit broadband Internet providers hasn't been, and never will be, very successful. Federal agencies, assuming they want CALEA to unambiguously cover broadband Internet access, including broadband in higher ed, should do the right thing and pass the necessary amendments to the existing law.
- Be sure to start with the basics – what's the Internet? What's a private network? What precisely is covered? What's not?
- And please, let's all admit reality: just as encryption was identified early on as something where providers simply couldn't do much, recognize that there may be other corner cases as well, and let's be realistic about what a provider can deliver in good faith. Advanced protocols should be exempted unless/until they begin to be exploited.

Financial Support Is Necessary

- Supporting lawful intercept isn't cheap. If lawful intercept capabilities are important, the government needs to step up and financially support that requirement – don't leave that burden on the shoulders of colleges, students and families.
- The original statute recognized the importance of financial support, and provided funding to underwrite the work which was required, but that funding dried up while CALEA-ifying the telephone system, and now funding isn't available for Internet providers (and colleges and universities) who must become CALEA compliant now. That MUST be corrected.
- The costs which law enforcement face also need to be recognized. It does no good to require providers and universities to build out lawful intercept capabilities if law enforcement literally can't afford to take advantage of the facilities we're collectively being made to install.

Give Broadband Providers More Time

- Recognizing that it took the better part of ten years to get most of the wireless and wireline telephone infrastructure CALEA-ready, it is unrealistic to expect broadband service providers and universities to be able to become CALEA-compliant at the drop of a hat.
- For context, note that the extension of CALEA to broadband providers was only contemplated in July, 2003 (see http://news.com.com/2100-1028-5056424.html); ACE vs. FCC wasn't decided until June, 2006; and the broadband CALEA technical specification, ATIS-1000013.2007, wasn't approved until April 2, 2007 -- yet all facilities based broadband providers were to be compliant by May 14, 2007!
- If you look at the implementation of CALEA as stretching back to the "dark ages" of 1994, that seems like an awfully long time to be working on building CALEA out, but in the case of broadband, we've only had a matter of **months!**

Leverage Lawful Intercept to Help Attack Cybercrime

- We're currently losing the war on cyber crime, and an important part of changing that dynamic may be beginning to more broadly use lawful intercept against cyber criminals.
- Currently lawful intercept is such a politically charged "third rail" (e.g., touch it and die), and so lumbering, many law enforcement officers won't even consider employing it, and thus cyber criminals are able to work online with impunity.
- Lawful intercept has long been associated with foreign intelligence and combating drug lords, but it needs to also be applied appropriately to the king pin cyber criminals who are destroying the usability and stability of the Internet, too. Existing laws (see 18 USC 2516) should be amended to allow the judicious use of lawful interception when investigating major DDoS and botnet-related cases, too.

Thanks!

- I'd like to conclude by acknowledging the thoughtful and detailed comments I received from a number of people who reviewed a draft version of this talk, including Jack Bates, Steven Bellovin, and Neil Schwartzman, as well as a number of additional individuals who either provided comments explicitly on a not-for-attribution basis, or who provided comments but didn't confirm whether they'd like to be publicly acknowledged or not. In any event, the content of this talk remain solely my responsibility.

- And with that, thanks for the chance to talk! Does anyone have any questions?