THANK YOU ALL. It is a pleasure to be here. The speakers on the earlier panel, who were all terrific and entertaining, are a tough act to follow. I hope I can be as entertaining and informative. Let me start by saying that I am not speaking for any specific client today.

This is a really interesting program title: “Service Providers Caught in the Middle.” I do not tend to think about it that way—being “in the middle”—I think it is just way too polite a term, way too generic, under-descriptive, and under-informed. Instead, I think “Service Providers As Piñatas” would be a better title because service providers get beat up by all sides all the time. While this topic is about service providers in the middle, I’m going to ad lib a little to play off of the question Kevin Bankston, of the Electronic Frontier Foundation (“EFF”), posed on the prior panel: “Where are the service providers?” As you will see through the following remarks, they are more on the front lines of these privacy battles than he or others realize and, in some cases, more so than the privacy groups themselves.

Remember, service providers are not in the business of electronic surveillance—they do not have a dog in most of the hunts over which they get beat up. And yet, they end up with the privacy community, users, and law enforcement pointing the finger at them as the solution to all of the privacy and security problems. Thus, on the earlier panel, Kevin asked, “Where are the providers?” Users ask, “Where are the providers?” Someone else will say, “They should be the last great shield,” while law enforcement says, “They are our most potent sword.” Well, in the law, which is really where we have to start and

* A. Gidari is a partner at Perkins Coie LLP where he leads the firm’s privacy and security practice. He represents communications service providers in the implementation of the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–21 (2000), and in responding to government demands for electronic surveillance. He most recently defended Google, Inc. against the Department of Justice’s (“DOJ”) demands for billions of user search terms.
end—we are in a law school after all—service providers are none of those things. They have, last time I looked, no line entry in any government directory; they are not an agent of any law enforcement agency; they do not work for or report to the Federal Bureau of Investigation ("FBI"); and yet, you would never know that by the way law enforcement orders them around and expects blind obedience. Likewise, they are not in the vanguard of privacy for their users or non-customer privacy advocates. They are neither formed nor organized for purposes of protecting user privacy, and, in most cases, the law does not require it.

Now I know that there are many laws with privacy in the name, such as the Electronic Communications Privacy Act ("ECPA"). But I would submit that anytime you see the word "privacy" in a statute's title, it is more about what you have lost than what you have protected. It is a little bit like environmental law—Clean Air Act, \(^2\) Clean Water Act\(^3\)—it is about how much you can pollute and not go to jail rather than about how clean you have to keep or make the air or water. Privacy is exactly the same way. We talk about ECPA as if it is a wonderful set of protections for users against misuse of their information by companies. Yet the simple fact is that under ECPA, a service provider may use your personal information, without any notice to or consent from you, and share it with anybody it so chooses other than the government.\(^4\)

How many of you are surprised to hear that? ECPA is, after all, a statute to protect privacy, and yet the statute unequivocally permits the service provider to do all of those things I just mentioned. What is more, ECPA permits the service provider to look at, access, review, and use internally all of your e-mail.\(^5\) Are you surprised by that? They do not have to give you notice of it.\(^6\) They can look at your e-mail, but disclosure of it to third parties is limited.\(^7\) ECPA applies to service providers "to the public," not private providers.\(^8\) For example, your employer is not a service provider to the public. Your employer who

---

8. Id. § 2702(a)(1).
receives e-mails from the public is perfectly permitted under ECPA to access, use, and disclose that e-mail.

So when we talk about the law and “service providers in the middle,” I suggest that there are no privacy restrictions for the most part on service providers. There are, of course, some minor exceptions in some industry “verticles,” like telephone records under the Telecommunications Act of 1996\(^9\) or medical information under the Health Insurance Portability and Accountability Act (“HIPAA”) of 1996,\(^10\) where health care service providers are more constrained.

What about the government, on the other hand? How constrained is it really? I would like to start this discussion by getting a sense of the general paranoia of the audience. The National Security Administration’s (“NSA”) warrantless surveillance program has recently become public, so perhaps everyone has good reason to be paranoid now. Let me take a survey anyway. How many of you think that every one of your domestic phone calls are being monitored by the government? [Question: Define “monitored.”] Intercepted. Every phone call in the United States domestically, not internationally, but domestic Portland to Seattle calls. I see a couple of hands—the truly paranoid are not afraid to be counted. How many think the government wiretaps more than 100,000 phones a year domestically under criminal statutes? That is a lot of hands, right? In fact, if you believe the statistics reported, in 2005, the total combined federal and state wiretap orders approved were only 1694.\(^11\) [Question: How many communications per order?] Well, I am glad that you asked that. In actuality, for each wiretap order approved, the average number of communications intercepted was 2835.\(^12\) Of those 2835, 629 resulted in incriminating interceptions.\(^13\) I love that number. Think about it. Any product manager would be fired in private industry if they only got a return on investment of one in four. One in four items sold! Of the total 4674 persons arrested (based on interceptions) at the end of 2005, only seventeen percent of those arrests resulted in convictions.\(^14\) Only 106 persons were convicted. It makes you wonder whether electronic surveillance really is effective.

---

12. Id. at 10.
13. Id.
14. Id. at 12.
These statistics come from the Wiretap Report, which is published annually by the Administrative Office of the United States Courts. It is well worth reading. The bulk of the wiretaps approved by state judges in this country occur in four states: California, New York, New Jersey, and Florida.\(^{15}\) Eighty percent of the state-level wiretaps occur in those states.\(^{16}\) Again, I am only talking about criminal cases. But for those foreign intelligence surveillance wiretaps reported, the number was not much greater—2072 in 2005.\(^{17}\) That is a grand total of less than 4000 wiretaps in the United States. Let me compare that with Germany. At a recent conference sponsored by Telestrategies regarding electronic surveillance, a German carrier representative said that over 360,000 wiretaps took place last year.\(^{18}\) I know we heard on the prior panel, from Lothar Determann of Baker & McKenzie, LLP, that electronic surveillance was not permitted under the German Constitution, so I am not sure under what basis they wiretap. But that is an incredible number. As an aside, I have a very good friend in Rome who recently remarked to me that his third wife left him when his conversation with his girlfriend, which had been taped, was disclosed—and he was a member of the police! I am told that they do 360,000 wiretaps in Rome alone each year.\(^{19}\)

I would submit that, globally, the number of wiretaps in foreign jurisdictions is significantly higher; indeed, enormously higher than in the United States. We actually have it better here than the headlines would suggest. I am not defending the government in their use of wiretaps or proposing that we do more of them. I am simply remarking on what the numbers suggest.

Returning to the Wiretap Report, the longest running use of wiretaps on a single order was in New York on a gambling investigation.\(^{20}\)

\(^{15}\) Id. at 7.

\(^{16}\) Id.

\(^{17}\) Letter from William E. Moschella, Assistant Attorney General, to J. Dennis Hastert, Speaker of United States House of Representatives (Apr. 28, 2006), available at http://www.fas.org/irp/agency/doj/fisa/index.html (see page 4 of the Foreign Intelligence Surveillance Act ("FISA") Index; follow “2005” link under the title heading “FISA Annual Reports to Congress”).


\(^{19}\) ISS World Conference, supra note 18.

It went on for 559 days. It was conducted by a joint task force of thirty FBI agents in Louisiana, lasted for many months, and required lots of resources. The average cost of a wiretap is about $70,000. So we know we are talking about big dollars over time here, right? What did they investigate? It was a wire fraud case also involving racketeering and money laundering. All sorts of suspicious financial activities. What do you think they monitored? A brothel in New Orleans. Now I wonder if their real interest was actually in all of those crimes. The reason they monitored the brothel was because they thought they would get people talking to prostitutes about money laundering and other illegal things. They hardly got a conviction, a prostitute for possession of marijuana. This is no joke. I am not making this stuff up.

Did I mention that I am from Seattle? Seattle is the birthplace of modern wiretapping. We claim that fame because the first wiretapping case to reach the United States Supreme Court occurred there in 1928—Olmstead v. United States. Olmstead was a case in the Prohibition Era of rum-running from Canada into Seattle. The conspirators were very successful people who made about $176,000 a month—a lot of money in the 1920s—running rum into Seattle. And they had a great scheme in order to do it because one of the conspirators, Olmstead, was the chief of police. Olmstead had his group of policemen assist him in getting the rum ashore and distributing it in Seattle. When one of the good cops thought he knew that a load was coming in and came down to the scene, Olmstead would immediately bribe him and get him into the conspiracy. By the time it was all done, he and twenty-six of his fellow officers were convicted on the basis of information derived from a wiretap.

The wiretap was in the basement of a warehouse on the shore where the rum would come ashore. The police wiretapped the basement and conducted a couple of months worth of taps to identify the scope of the scheme and the participants. This operation was in violation of a 1905 Washington law, which actually prohibited the inter-

22. Id. at 11–12.
23. 277 U.S. 438 (1928).
24. Id. at 456.
27. Id. at 457.
28. Id. at 456–57.
ception of telephone communications. How many of you know the outcome of that case? The outcome is really interesting because we take so much for granted today about what our Constitution says and what is and is not prohibited under it.

In 1928, Justice Taft, who wrote the *Olmstead* opinion, asked: What expectation of privacy could anyone have in their voice projected over a wire outside of a building? None whatsoever in his view. There could be no search or seizure of a telephone conversation that implicated Fourth Amendment concerns at all, according to Justice Taft. That was the status of the law until Congress passed section 605 of the Communications Act in 1934, in which Congress made it illegal for any person to wiretap. In subsequent cases, the Supreme Court read section 605 to provide that the definition of “any person” included law enforcement, making it illegal to wiretap at all.

Many people recognize *Olmstead* because of Justice Brandeis’s incredibly prophetic dissent. I am spending some time on this, not because I think the case is incredibly important for what we are going to talk about now, but because I think it is a very interesting stepping stone to it. I want to read Justice Brandeis’s quote because it really echoes today, in terms of how you think about the NSA warrantless surveillance program, wiretapping in general, and the so-called “surveillance society.”

The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.

29. *Id.* at 468.
30. *Id.* at 455–69.
33. *Id.* § 605(a).
34. *See*, e.g., *Benanti* v. *United States*, 355 U.S. 96, 100 (1957) (holding that evidence obtained in violation of section 605 of the Communications Act of 1934, 47 U.S.C. § 605, whether by state or federal agents, is inadmissible in federal court); *Nardone* v. *United States*, 302 U.S. 379, 384 (1937) (holding that in light of the provisions of section 605, evidence obtained by federal agents in violation of section 605 is not admissible in a criminal trial in federal district court).
35. *Olmstead*, 277 U.S. at 474 (Brandeis, J. dissenting).
And that was in the 1920s. Think how prophetic those comments are today now that we face new and incredibly capable surveillance tools, like thermal imaging. Just a few years ago we talked ominously about “Carnivore,” a wiretapping mechanism for the Internet, which is basically a large vacuum cleaner that sucks up all of the digital bits for others to analyze. These tools are truly amazing. Justice Brandeis was a prophet.

But who do you think stood up in this case and filed an amicus brief arguing on behalf of Mr. Olmstead? It’s remarkable. AT&T. How ironic that eighty years later they would be on the opposite side of this issue. They argued in Olmstead that “[t]he telephone has become part and parcel of the social and business intercourse of the people of the United States, and the telephone system offers a means of espionage compared to which general warrants and writs of assistance were the puniest instruments of tyranny and oppression.” What a remarkable statement in juxtaposition with where AT&T apparently stands today on the NSA program.

So, in my estimation, service providers have had a pendulum swing. And they are on, I would submit, the opposite end of the pendulum than they were eighty years, sixty years, fifty years, and even ten years ago. There are a lot of reasons for that. September 11 changed a lot of things. It changed a lot of things for service providers. And it changed a lot of things for the government in terms of how they look at things. I want to just talk for a few minutes about some of the changes that are not reflected in law or written about much.

One thing that has changed with law enforcement is their patience. The government no longer is patient with service providers who delay, argue, review process, complain about it, or push back. Just the opposite—“impatient” is one word that comes to mind. Bullying is another. When Kevin Bankston of the EFF asks where the service providers are or have been, I know at least where I have been. I have been in court twelve times in the last year responding to orders to show cause in contempt proceedings. I have had one corporate client actually convicted of criminal contempt for failure to provide call records in a timely enough way that the judge could complete his investiga-

37. See, e.g., Leslie Cauley, NSA Has Massive Database of Americans’ Phone Calls: 3 Telecoms Help Government Collect Billions of Domestic Records, USA Today, May 11, 2006, at 1A.
tion. My client was told that if the company ever again failed to be timely in the production of those records, he would be the one that would go to jail. If patience is a virtue, then the government is no longer virtuous in these cases.

In spite of the lack of patience or tolerance for resistance, I have been on the proactive side for service providers. Let’s specifically talk about location tracking—the ability to track a wireless device in real-time. The law today is still not clear as to the legal standard necessary to obtain real-time tracking information. Is it probable cause, or is location data treated like stored transactional information under section 2703(d) of Title 18 and, therefore, subject to a lesser standard? I bear some of the responsibility for the continued muddle. In 1994, I worked with the DOJ to get to the middle ground, which was the lesser standard, in an effort to get a compromise that would get carriers out of the business of going to court over every order. Because a 2703(d) order still required a judge to make specific findings and therefore review the law and facts, it seemed like a good compromise at the time.

But in 1994, the law certainly was not clear. Who is really to blame in this? It is an interesting discussion. Location information, prior to 1994, was treated as basic subscriber information and could be obtained by the government on a mere subpoena. Then Congress passed the Communications Assistance for Law Enforcement Act ("CALEA") in 1994. In that law, Congress amended ECPA by dividing subscriber information into two parts. One part referred to basic subscriber information: your name, address, phone number, and calling records, essentially. The other part addressed “other information,” which included things like clickstream data, even though there was not really a robust Internet back then, and cell site location information.

In the legislative history, Congress specifically referenced the cell tower or location information of cell phone communications as falling within the second category. That information, it said, could only be obtained with an order issued under section 2703(d), based on “spec-

41. Id. §§ 2703(c)(1)(A)–(B) (2000).
42. Common examples of “record[s] . . . pertaining to a subscriber” include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and e-mail addresses of other individuals with whom the account holder has corresponded. See H.R. Rep. No. 103-827, at 10, 17, 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511.
specific and articulable facts" that the information was material to an ongoing investigation. So where were the privacy groups then? Supportive of that new standard? Yes, they supported it, advocating in favor of the higher standard that required an independent magistrate rather than somebody signing a mere subpoena to get that information. As added protection, the privacy groups convinced Congress that it was not enough to get location information on a ministerial pen register either. CALEA specifically carves location information out of other information that can be obtained solely pursuant to a pen register order.

*In re Grand Jury Subpoena to Southwestern Bell Mobile Systems, Inc.*, decided in late 1994, was the first case to involve location information after Congress passed CALEA. An Assistant United States Attorney issued a subpoena for location information. Southwestern Bell refused to provide the information based on CALEA. So where was the service provider? In the middle again, and this time in federal court in Kansas City. We fought the subpoena and the DOJ eventually withdrew the order to show cause as to location information because the DOJ recognized that they had to show the higher standard under section 2703(d).

Let us look at this location issue more closely. Location is just data; it is a signal that flows through the wireless network. It is the evidence of the connection of your cell phone to a tower that tells all of your friends, "Here I am, route the call to me." It works that way when you are in Texas and when you are traveling to Seattle; it is a signal that is registered in the system of the network to say, "Here I am."

In 1994, it was there to say, "Bill me extra because I am roaming." At that time, there were no truly national networks. So location would register on a cell tower every seven to ten seconds—what is called "au-

---

45. *Id.*
48. For this reason, there is no published record on the location information issue; the case went forward on another issue—the definition of toll record—demonstrating again that service providers are more than in the middle. They are often in court.
tonomous registration”—and then, when the phone is actually con-
nected, that signaling information gets recorded for purposes of
billing.

Today the service provider stores the cell tower registration infor-
mation. In essence, it becomes historical, transactional information
within a millisecond of when the provider receives it. The process pro-
vided under section 2703(d) is the correct way to obtain stored trans-
actional records. But what happens when law enforcement wants that
location information every few milliseconds? The answer is that they
want a “poor man’s wiretap,” because if they try to get transaction
records every five seconds then what they are really doing is real-time
tracking, not accessing stored records. So maybe Congress meant for
law enforcement to be able to get historical stored location informa-
tion but not to actually track somebody as they move, at least on a
standard that is less than probable cause.

That is a fair enough argument in a vacuum, but the service prov-
iders never made it. The compromise I mentioned between the carri-
ers and the DOJ gave real-time location tracking on a 2703(d) order
because the service providers were beaten up so badly by law enforce-
ment demands in the years following CALEA. No one wanted to be
hauled into court on a show cause order. Besides, location tracking
has become an enormously successful law enforcement investigative
tool. It finds kidnappers. It finds people lost on the side of the road in
snow storms and in mountains. It finds people doing things they
should not be doing. It is a very useful tool.

I joke a lot about how good a tool it really is. One of the first
recorded instances of location tracking that I am aware of was in the
mid-1990s in Chechnya, Russia, where a Chechen army general was
upset about politics I will not go

In order to negotiate a com-
promise of a revolt that he was leading, the general was having a satel-
lite phone conversation with the Russian Parliamentary leaders. As he
was sitting out in the field having this discussion, two surface-to-air
missiles landed on him and ended the conversation. Location technol-
yogy in wireless phones is a remarkably effective tool. I do not know
what legal process the satellite provider got.

Location tracking was also a useful tool in the early days of Mc-
Caw Cellular, which became AT&T Wireless and ultimately Cingular,
because when cell phones were introduced, almost seventy percent of

49. Patrick S. Radden Keefe, Chatter: Dispatches from the Secret World of
the calls made in the New York market were being made fraudulently. In the old analog cellular days before there was authentication, your cell phone could easily be “cloned” by bad people. You could go through Manhattan and follow these so-called “call-sell” operations where people who cloned phones would stand on the corner, talk on the phone, and sell you five minutes of time for ten bucks to call anywhere in the world. You could follow the calls right around the globe in the network operations center of the wireless carrier.

So McCaw Cellular would put a cell-site emulator on top of a van, drive around Manhattan, technically use the emulator to locate and identify a call-sell operation, and then call law enforcement. The police would come in and bust the operation.

Indeed, wireless carriers found lots of useful applications for location services. Today, we have robust location-based services that include programs like “Family Finder,” which is offered by Sprint/Nextel to its subscribers. You can get four phones for your family and give one to each of your kids. When they go to school, a text message will be sent that says, “safely arrived at school.” When they break the “virtual fence” around the school, another message will be sent that says, “your kid is sneaking out of school.” And if you do not tell your spouse that it is on his or her phone it can be highly instructive. Why am I off on this tangent? Because it raises the issue: What legal process is required in a divorce case or an insurance case in order to get location information?

If law enforcement can get location information on a section 2703(d) order when it is stored, yet needs a search warrant when it is real-time tracking (if the privacy advocates are correct), what legal process is necessary in a civil case? What is this Family Finder service governed by? Well, ECPA does not answer it expressly. Or it does, if you listened to what I said at the outset—a carrier may disclose any transactional information to any non-governmental third party without any legal process, without notice, and without consent. That is what ECPA says. It is a little odd that we talk about imposing a higher standard on the government for one of the most essential investigative tools they have in their arsenal for finding the bad guy, and yet we let service providers just hand it over to anyone, use it, give it away, play with it, and do whatever they want—without any legal process whatsoever.

So where are the service providers on this one—in the middle? Not at all. They are out front making money introducing great new services and using identical information, without any legal bounds whatsoever, that some would deny law enforcement access to without strict legal procedures. This is interesting because some states are introducing new laws for things like event recorders in cars. Legislators apparently do not want the rental agency knowing when someone goes beyond the 100-mile limitation in the contract. Or, with location technology, providers can also measure speed and direction. Indeed, there are new applications being purchased by the Department of Transportation that actually are used for force planning, evacuation, and other issues based on partnerships with carriers looking at aggregate location information.

For example, remember a cell phone registers on the network every few seconds. So, if a carrier provides the autonomous registration of all of the users on Interstate-95 driving north or south out of Washington, D.C., one can actually measure and triangulate the speed and direction of traffic down I-95. I can tell if the highway is a parking lot. I can tell if arterial roads are open. This is a new application. And there are applications being introduced all the time.

So what does a service provider do when a third party asks for location information? They get sued regularly now for this information. I do not know what the right legal standard should be for location information for either civil cases or criminal investigations.

The privacy groups have a good argument though. As Kevin Bankston described in his presentation, Magistrate Judge Smith in Texas articulated the history of the law well.51 I spent about two hours talking with Judge Smith before his second opinion on location tracking, and true enough, he is a maverick. His judicial opinions are worth reading. He really has led a mini-Magistrates’ Revolt to say, essentially, “I’m tired of reading these pen register orders that ask for location tracking on a less than probable cause basis, and I’m going to do something about it.”

So where are the service providers after Judge Smith’s opinion? After Judge Smith issued his order, one of my clients got a second order from the magistrate sitting immediately next to Judge Smith, demanding the location information in a pen register order. Again, where is the service provider? We filed a motion and said we had to

51. See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005).
move to quash this order because in this Texas district, surely one magistrate's opinion is binding on the other magistrates in the same district, right? I think there are thirty of them in that district. The answer is, "Wrong." One magistrate's opinion is not binding on another, and as this second magistrate put it: "Are you giving it to me or not?" We were thinking about it, and as the lawyers were on the phone in this case and not in the court room, we knew we could not be put in handcuffs, which is very important, so we pushed back a little. The magistrate had none of it. She ordered the location produced or else. So it is an interesting position that the service providers often find themselves in.

Let me talk about a few other areas and how the service provider is in the middle again. For example, how many of you realize that a law school is a service provider? The University of San Francisco is now, by Federal Communications Commission ("FCC") decree, a broadband service provider who has an obligation to ensure that all of your student and faculty communications are wiretappable.\textsuperscript{52} Thank Congress for passing CALEA, which requires on its face that telecommunications providers make their networks wiretappable.\textsuperscript{53} For the first time in the history of this country, we basically mandated, to paraphrase former Director of the FBI Louis Freeh, "seatbelts for carriers."\textsuperscript{54} Public safety demands, because of new advancements that have moved communications across multiple networks, that we require service providers to design in—to "bake in"—wiretap capabilities from the outset into their systems.

I might add that this was done with the complicity of the privacy groups who compromised on that legislation. Lee Tien—who has worked with EFF since its inception and is sitting in the front row—will of course argue with this because EFF broke away from those other privacy groups as a result of CALEA. But in fact, CALEA was a compromise. The privacy groups said, to paraphrase, "that it is really hard to fight about this surveillance stuff. Law enforcement has a legitimate need, and it is really hard to get this information with all the advancements in communications networks." So they compromised, and we got CALEA.

\textsuperscript{54} Joint Hearings on H.R. 4922 and S. 2375, supra note 44.
CALEA took four years to implement for traditional carriers. The law provided that the method and means to conduct the wiretap would be done through collaboration with carriers and their manufacturers in developing standards for wiretaps because industry would know best how to design a solution.\textsuperscript{55} So industry created a standards process. And I was lucky enough, or unlucky enough, to be one of the only lawyers who, for four years, sat with about sixty engineers, once a month for as long as a week at a time, to develop the standards. As an aside, I have heard every bad lawyer joke that could ever be dreamed up by engineers. Engineers are not funny. I started billing them for reading the lawyer jokes.

During those meetings, the service provider was in the middle thanks to the standards process in CALEA. The service provider industry's interest in those meetings was to keep the standard simple and elegant and therefore cheap and easy to implement. We got it mostly all wrong, and I will come back to why we got it all wrong in a minute. Let me observe first that there were no privacy groups in those meetings. They were open meetings, they could have attended, but no privacy groups sat in on the standards meetings. For four years we negotiated over what capabilities were required and what CALEA required industry to do. We had a lot of legal discussions, including three legal summits with the FBI.

Some of my experiences were priceless. The biggest fight was over location. We did not want to give it to them because it did not seem to be within the definition of call-identifying information, and it was really hard to separate it out and deliver it when it was not associated with an ongoing phone call—the autonomous registration information I referred to earlier. So we argued for CALEA to exclude location. It says it on its face in section 1002(a)(2)(B), "such call-identifying information shall not include any information that may disclose the physical location of the subscriber,"\textsuperscript{56} so we were not going to build in a location capability.

At a standards meeting, an FBI agent, who attended and was a chief spokesman at the meetings, took his handgun out, slammed it on the table and said, "You people support the pornographers and drug dealers. Do you understand why we need this?" This is no joke. This is how the standards meetings went for four years as carriers were caught in the middle.

\textsuperscript{55} H.R. REP. NO. 103-827, at 10 (1994), reprinted in 1994 U.S.C.C.A.N. 3490 ("The bill allows industry to develop standards to implement these requirements.").
Ultimately, we passed a standard that excluded location. The FBI and DOJ appealed that standard. CALEA permitted a process where you could challenge a standard if you believed it was inadequate and did not provide all the capabilities that CALEA permitted. We went to court and we won, remarkably enough, on six of the features we said were not required to be in the standard. We lost on location. The Court of Appeals for the D.C. Circuit said that location was included in the definition of call-identifying information—otherwise why exclude it on pen registers expressly? They dodged the question of the legal standard, though, because all the standard says is that a provider must give location information when appropriate legal process is given. The issue was not really ripe to argue about because nobody was saying that appropriate legal process is not required by the carriers. So location stayed in the standard.

So what does the standard do with respect to location? All of the manufacturers for telephone companies build in the automated disclosure of call identification information for each call as it occurs. And they do this with parameters that include each of the data elements when a triggering event occurs. So what did they do with location? They made it a parameter of every phone call when a call is initiated or terminated. Location is a tag-along parameter whenever there is a trap, trace, or pen register order. Not a tracking order alone, though. There must be a phone call in order to provide location under the standard. So why is this wrong? Because the government does not always have a combined pen register, trap, and trace order; sometimes they ask for location alone, and in that case they will get all the numbers dialed too, which may not be authorized at all. And in any event, today, under every single pen register order implemented, they get pen register, trap, and trace.

And under every pen register order implemented, the government gets location. They filter it out on the other end, or at least they are supposed to. Some of the manufacturers built a toggle that allows carriers to flip a switch and not provide location if they do not want to. But some carriers just do not know. Not all carriers are as big as Ver-

59. USTA, 227 F.3d at 463.
60. Id. at 463–64.
61. Id. at 463.
62. Id. at 465.
63. A pen register captures the numbers dialed by the target; a trap and trace captures the incoming numbers from someone calling the target.
izon. Not all carriers have a lawyer who knows anything about electronic surveillance or CALEA. By the way, how many carriers do you think there are in this country? Would it surprise you to know that there are at least 3500 registered carriers in this country? There are another 1300 wireless companies. Hard to believe there are that many, is it not? Outside the top fifteen or so companies, these carriers do not have lawyers. When they get an order, they're not calling me up and asking my advice. They're not calling up Kevin Bankston or other privacy groups and asking their advice. They are just doing it. They are paying a fortune for the CALEA hardware and software, and they are not paying to filter it further. The location information is just flowing as part of the solution. This is all a little remarkable, is it not?

So what is that small service provider in the middle supposed to do? Challenge the federal government, say no, and go to court? Or are we really saying the responsibility of the service provider in the middle is applicable only to the service provider at the top? The top five carriers, maybe. Are they the ones who should do it? Because, after all, the big carriers have the most money, time, and lawyers.

How does that sit when you are a multipurpose phone company and your general counsel is the former Attorney General of the United States who was responsible in that job for implementing CALEA? I'm referring to Verizon's General Counsel Bill Barr. Verizon is not likely going to see these issues the same as Mr. Bankston.

Besides, carriers are not paid to buy or install this equipment. In the case of wireless carriers, it costs somewhere on the order of a billion and a half dollars to implement CALEA across the industry. That is not a small amount. So where are the carriers? They are paying a significant price for public safety. I note that the industry had to implement a second round of changes to that standard after it was challenged, and they were not compensated for that either.

Now we have the Internet. We have all of your voice communications moving to Voice over Internet Property ("VoIP") communications—packet-based rather than circuit-based calls. I think it is really interesting to have a little discussion about location in that context. Where are we going to be with location in a packet world? When you are on the Internet, does anybody know who or what or where you are? More or less. We can find an IP [Internet Protocol] address and then trace that IP address back to an Internet Service Provider ("ISP") who may or may not have information about your identity as a subscriber. Typically, if you are paying for service, the ISP will. And the
ISP will know where you live and so on. And so at least we'll be able to go back and find that person.

What about services like Skype? Off-shore based, peer-to-peer, VoIP communications. With Skype, I no longer have any ability to know where the user is located. Look at Vonage on the other side of the VoIP equation. It is an infrastructure-based voice provider in the United States. It is not peer-to-peer, but rather interconnected with the public-switched network. That should help law enforcement know where you live if you are using a VoIP-enabled phone and Vonage service. However, all it can tell you is where the ISP is located. What's the problem with that? If I have a Vonage phone, work for a large company, and dial 911 on my VoIP phone while sitting in my office, what it looks like on the receiving end at emergency services is that the call comes from the company's campus. Now, I take that phone with me on vacation to go fishing in Montana, plug it in at my wired cabin, and dial 911 because I am having a heart attack. Where do the police go? To my workplace campus because that's what the originating location looks like in a VoIP call—the number assigned to that desk.

Well, what about location? Should we not require a VoIP provider to identify itself and where the caller is located for 911 purposes? This is an insidious approach, right? It is about public safety and emergency services. The answer is yes, of course. And the FCC has mandated it. Location is required, and the FCC adopted an order to explore in more detail how providers can technologically do it.64 But once they do it, what happens then for law enforcement purposes? I will now be able to track you and your VoIP calls and get your location. Now that's not necessarily a bad thing or a good thing. What's the law that will apply if I want that information? A warrant? Or will it always be registered and historical with a 2703(d) order only? The government's position will be that all they need is a section 2703(d) order, at least if it's historical and combined with a pen register for tracking, to find out which Starbuck's coffee shop you are in when making a call.

Let me come back to college for a minute and CALEA. I said CALEA applied to telecommunications carriers. The statute says that it applies to telecommunications carriers who are providing services to the public for a fee, but does not apply insofar as they are providing

information services. Now I do not want to get too deep on the difference between telecom services and information services, but they are very different entities.

CALEA defines a telecommunications carrier much the same way as the Telecommunications Act of 1996: An "entity engaged in the transmission or switching of wire or electronic communications as a common carrier," including commercial mobile wireless services. However, the definition under CALEA also includes any entity engaged in a communication service, if the FCC finds that (1) the service is a replacement for a substantial portion of the local telephone exchange service, and (2) it is in the public interest to deem such an entity to be a carrier under CALEA. It is this definition that the DOJ and the FCC relied upon to extend CALEA to internet communications and that the Court of Appeals for the District of Columbia affirmed in June 2006.

An information service makes some computer-processing application or service available to an end user via telecommunications. One example of an information service is electronic messaging, like e-mail or instant message. In contexts other than CALEA, the FCC has declared broadband internet access to be an information service. Historically, the FCC has not regulated information services. However, the FCC has applied a different definition under CALEA and determined that the telecommunications component of an information service is covered by CALEA while the remainder of the information processing is not. The Court of Appeals upheld the FCC's definition in its June 2006 opinion.

The FCC concluded that all broadband, all facilities-based broadband internet access, and VoIP services are covered by CALEA, and must, by May 2007, have all of those capabilities I was talking about a few minutes ago baked into the routers and servers that give you access to the Internet.

This had some unintended consequences. Some did not know they were a service provider under that definition. Who provides you access to the Internet? Your school does. Libraries? Businesses? Corporate networks? All of those entities meet the FCC's definition.

---

66. Id. §§ 1001(8)(A)–(B)(i).
67. Id. § 1001(8)(B)(ii).
68. Am. Council on Educ. v. FCC, 451 F.3d 226, 234 (D.C. Cir. 2006) (reasoning that the FCC is entitled to analyze the statute and apply it under Chevron USA v. Natural Resources Defense Council, 467 U.S. 837 (1984)).
69. Id.
There's an exemption in CALEA for private networks. The FCC looked at that and said a private network is one that does not cover or connect to the Internet. But, insofar as the private network uses or supports the connection to the Internet, it is deemed a public provider. The universities are on the hook and in the bulls-eye now.

So by May of 2007, your e-mail from your desk, in your dorm, and from your library, must be amenable to interception by the government under proper order. And if it is an improper or questionable order, what will your university legal department accept? So now you are in the middle too! It is no longer AT&T or Verizon or Cingular or Google. It is you. You are in the middle. And what is your university going to do? Which State Attorney General is going to stand up for a state college and say you have given the school an improper order? None. You know why? Because they represent the agency issuing the order. The last time I looked, the police worked for the state. And the very same lawyers will have to review the order that the law enforcement agency issued. So that service provider in the middle is not going to be saying very much.

I do not know where the universities will come out on this and how or whether they will implement CALEA and its requirements. Now you are sitting back saying, “Alright, great. I’m just going to go down to Starbucks to download my music and I’ll be fine. I'll get on the Wi-Fi connection there, or I’ll go over to Mountain View where they have municipal Wi-Fi for free.” But all broadband internet access is covered by CALEA. Wi-Fi is not excluded. Municipalities who offer it are also the ones who will issue the orders to wiretap it. The city as service provider is again in the middle. And I do not expect them to stand up and argue that their law enforcement agency is wrong in issuing the order.

Let me round out this discourse with a few more observations on providers in the middle. I went through the Wiretap Report with you a little bit earlier, and Kevin Bankston was right when he said we do not know how many pen registers or trap and traces are conducted each year. We should. The statute actually requires the Attorney General to annually report this information to Congress. Every year in April after the Wiretap Report comes out, I call the DOJ and ask them for the pen register report. I do not get it. They do not do it. So where are the

---

70. Since this speech, many universities have concluded that they are exempt private networks, but others have decided to comply.
71. CALEA ORDER, supra note 52, at 13–14.
privacy groups on this? Where is the Freedom of Information Act request? Where is the lawsuit for that information? How many pen registers do you think are conducted? Let me put it in order of magnitude for you. A wireless carrier with twenty-million customers has an annual operating budget for its securities group of about three and a half million dollars. It employs over thirty people in responding to government requests for information. It handles on the order of 500 requests for customer records per day; ten or more pen register requests per day. If you multiply that number across the 200 million wireless subscribers who are out there, you get a rough order of magnitude with how many pen register orders we are dealing with a year. There's also a little bit of a hint of it in the FBI's filings in CALEA. By my count, at least prior to September 11, it was probably somewhere in excess of 60,000 a year. And that 60,000 per year is an ongoing recording of every number dialed or received by the person under surveillance for sixty days or as long as the order is expended.

Let us look at another basis under ECPA for disclosure of information voluntarily. What about emergency requests? When the federal government calls and says, "There will be a bomb going off in the District of Colombia in two hours. I need this subscriber's information," what do you think the carrier is going to do? Exactly what the law permits them to do in an emergency—to disclose information, the content of a communication and a customer record, to any law enforcement agency for the purposes of an emergency. Those numbers are not tracked. Those are not reported. There is no reason to follow up with a subpoena or order to document it. It is an emergency. After September 11, emergencies went through the roof. My clients respond to, on the order of, about a hundred a month. That's a lot of undocumented requests. What are service providers going to do? Say no? Tell them to go to court, bring a motion for contempt, and they'll respond in due course? In the meantime, the World Trade Center comes down. Now there's a headline: "Carrier failed to give over customer record one hour prior to planes hitting tower." It is just not going to happen. In every single case, as the law permits, the service provider will give that information over. And they will do that internationally as well as domestically.

74. 18 U.S.C. §§ 2702(b)(8), (c)(4) (Supp. 2006).
Service providers are in the middle globally. Prior to the reauthorization of the USA Patriot Act in March 2006, service providers were a little torn on this issue of disclosing information in an emergency situation to foreign governments. You might understand why, because some foreign governments might lie. It might be more about suppression of speech in China than it would be about bombing a subway in Madrid. And the service providers were always a little cautious about being in the middle of that sort of discussion. Then comes along the USA Patriot Act, and in its reauthorization, it provided that in an emergency you may only disclose information to a federal, state, or local law enforcement agency. Prior to that, a service provider could help out with that bombing in Madrid, and it often did. As a result of post-Patriot Act reauthorization, foreign governments actually have to come to the United States in an emergency—the DOJ gets the intelligence of what is going on in that country, and the service provider discloses the information to the DOJ, and then they give it to the foreign government.

How many of those requests do global providers get? Anyone read about Google in their fight with Brazil? This stuff is not in the mainstream press. Orkut is the Google equivalent of MySpace. Orkut is a social network that is wildly popular among the Portuguese in Brazil for some reason, nobody understands why. There are over seventeen-million users in South America, mostly in Brazil. And the Brazilian government does not like skinheads, they do not like neo-Nazis, and they do not like child pornographers. And those seem to be the largest user groups of Orkut! So, the Brazilian prosecutors threatened to incarcerate Google Brazil’s sales manager in their marketing and sales office in São Paulo if Google did not disclose all of the Gmail associated with the Orkut user accounts and all the customer information held by Google, Inc. in Mountain View. Can Google do that in response to a Brazilian court order served on a marketing and sales agent in São Paulo when to do so would violate United States law? Well, there was a compromise, and Google did disclose some information, but not content. This is all public record; you can go “google”

“Google Brazil” and come up with it. And so they have provided cus-
tomer information and information that was otherwise publicly avail-
able, and there is a tenuous compromise with Brazil. But I think it is
interesting when you think about how global this has become with the
service provider in the middle. Are they supposed to then fight Brazil?
India just showed up with the same issue. What are they supposed to
do in those situations? It really has become a global problem.

Now the United States, of course, has had no problem for years.
If anybody has read the case, *In re Grand Jury Proceedings Bank of Nova
Scotia*, the United States feels that the foreign law’s jurisdiction is
irrelevant. If there is an agent, a director, or an officer in this coun-
try, the company can be compelled to disclose bank information even
though it violates bank secrecy laws of the country where that entity
and the records are located. So there really is not all that much differ-
ence between the United States’ and the Brazilian government’s posi-
tion. It is equally interesting vis-à-vis Europe that the United States
companies are saying, “Trust us. We are under Safe Harbor [referring
to the European Union Privacy Director and the compromise to per-
mit personal information to be sent to the United States]. Send per-
sonal information out of Europe to us in the United States to process.
It is more efficient. It is more cost effective. We’re trustworthy compa-
nies.” But, do not let the European Union law enforcement agency
come calling to get that information back because we cannot give it to
them. Law enforcement does not like that. We will be fighting those
agencies forever. Well, it is not an easy issue to solve.

What service providers would like is to be out of the middle, but
in my view, it is not going to happen. They are always going to be in
the middle. If they cannot be out of the middle, what they would like
at least is full immunity. I know some people are unhappy hearing
about proposed legislation to resolve the NSA warrantless spying mat-
ter because one of the provisions in it is to retroactively absolve any
service provider who cooperated in that program and to give them
immunity. I represent some people in that process so I cannot com-
ment on what is good or bad about it, but I will tell you that the exis-
tence of immunity reduces the carrier’s incentive to say no. When
there is immunity and it is comprehensive, why does a carrier spend
any time reviewing an order? So if that is not going to work for a

---

78. 740 F.2d 817 (11th Cir. 1984).
79. Id. at 832.
80. Note that this particular provision of the Electronic Surveillance Modernization
Act, H.R. 5825 was not passed.
carrier, even though they want that, from a policy point of view, what else could we align that would make carriers more responsive to Kevin Bankston’s concerns and those of other privacy advocates? How about compensation?

Compensation generally equals sunshine and transparency. Currently, if service providers are not paid to implement wiretap solutions, if they are not paid to produce thousands and thousands of records, there is no audit trail. And if there is no audit trail, there is no visibility and transparency into how the money is spent, and you do not know what capabilities are actually being acquired. So, carriers like compensation because they get paid. They like to have those thirty people answering subpoenas, at that one wireless carrier I mentioned, with the three and a half million dollars a year going out the door, compensated for what they do. That would be a good thing. Transparency would be a good thing. You do not think so? You think it should be free? [Comment from audience: “Well, I’m saying that if it’s going to be paid for, then there’s even less incentive to not do it, because at least now it hurts your bottom line.”] That’s fair enough. I do not disagree with you on that one at all. But three and a half million dollars at Google is nothing—by the way, Google is not the one I was referring to—three and half million in companies with revenues that are in the billions is meaningless. There is no disincentive there at all. My point is a simple one. It is transparent and traceable. When I can follow the money, I know how much of something is being consumed—how many wiretaps, how many pen registers, how many customer records. Couple that with reporting, and at least you have the opportunity to look at and know about what is going on. Because right now, you do not know.

I want to close with one more example. While we cannot talk about specific wiretap orders, nothing prevents me from talking about specific content of those orders in a general way. With respect to location information of specific users, many orders now require disclosure of the location of all of the associates who called or made calls to a target. The law again says, provide location information when there are “specific and articulable facts” to believe the user’s information is relevant to an ongoing investigation.81 How is a phone call to an unknown associate material when you do not know that the call is even going to be made before you sign the order? How is there any connection at all? It could be the pizza delivery man being called. So now we

have location being delivered on each and every one of those individuals. And to mine that data, carriers have to dig really, really deep in the switches to get it. They are not allowed to be paid for it, according to law enforcement, because this is a call record under section 2706 of ECPA for which no reimbursement is authorized. What would paying do? It would actually provide a trail, and perhaps if they had to pay the actual cost, it would actually deter them from the “tragedy of the commons” or the “tragedy of privacy,” whichever way you want to look at it, from over-consumption. Right now in the world of surveillance and data collection, because we suffer from an incredible amount of over-consumption, it is the service providers who are in the middle serving up that data.

Thank you for giving me the opportunity to have a wide-ranging discussion of the issues facing service providers who are caught in the middle each day between protecting the privacy of their customers, following the law, and meeting law enforcement demands.

82. 18 U.S.C. § 2706(c) (2000).