Modern Communication Protocols Treatment Under the Electronic Communications Privacy Act

Barnaby M. Page
January 2011

Abstract

The modern communications explosion enables consumers to stay in touch with family, friends and co-workers across multiple different devices. The method of communication that users choose, determines the level of privacy that the law will accord the users transmissions and documents. Our thoughts and words move at the speed of light and circle the globe but should we sacrifice our privacy simply because technology has broadened our options beyond the pen and paper and a desk in our home? These issues touch all Americans as well as corporations which are moving operations to cloud based services. This paper looks at the most commonly used protocols and assesses privacy levels as compared with traditional telephony.

1. Communication in the Modern World

Every day, individuals utilize many different communication protocols in order to perform tasks on the job or to talk with friends and family. Our telephones are predominantly "wireless," with many people opting not to purchase a "landline" phone at all.[1] Mobile handheld devices are "smart" because they combine telephone calling with email, texting, instant messaging, web browsing, point of sale capability.[2] Indeed, it seems each month, a new feature is added.

The ubiquitous nature of the smart phone in today's work environment means that everyone is doing some private communication while at work. A parent talking with his child at home does not expect that anyone is listening. The conversation remains private. But as soon as that parent chooses to use a communication device, just like the employee's choice to use his smart phone, that conversation includes a third party. That geographic distance forces the use of a digital device raises concerns about privacy. The law characterizes most communication technologies by use of three major categories under the Electronic Communications Privacy Act (ECPA).[3] This paper focuses primarily on the network-based protocols under Title II of the ECPA, also called the Stored Communications Act (SCA).[4]

An understanding of how each of the communication devices processes its information is fundamental to determining which federal statute controls. Some of the key differentials include: whether the communication is continuous and unbroken, stored en-route between sender and receiver, held for a certain period of time, audible or contains information that holds the purpose of making the communication (content) or is merely connection information that facilitates delivery of the communication (non-content).[5]

At first, it seems easy to assess from a technical perspective but a merger of different technologies since enactment of the SCA, combined with a shift in the way people choose to communicate their most private thoughts, complicates the assessment. What's more, users probably do not realize how their communications actually traverse the networks, making their way to handheld devices

or laptop computers. A brief discussion of the technology protocols assists in understanding if maintenance of the letter and spirit of the original legislation during the world's explosive communication growth survived.

In addition to the ECPA, the post 9/11 USA-Patriot Act and its amendments to the Foreign Intelligence Surveillance Act (FISA), complicated the courts' ability to determine the existence of violations of the Fourth Amendment right to privacy. The government obtains information from these new technologies and the networks that service them. This paper discusses how modern communication protocols operate and integrate with traditional telephone network privacy under the ECPA, as amended by the USA-Patriot Act and considers FISA in relation to the government's ability to monitor domestic communications.

Present day telephones are digital and tie into the public switched telephone network (PSTN). The PSTN includes cellular, satellite, cable, telephone lines and microwave relays and became almost entirely digital over the past 20 years.[6] The move to digital enabled telephone companies ("telcos") to offer rich features such as full motion video, direct to subscriber homes.[7] Additionally, the Internet and its growth, led the telcos to adopt the packet switched network approach.[8] Instead of connecting one phone number to another phone number with a switching router, a packet switched approach enables the telephone caller sessions to be split into packets and sent to an end point where they are re-assembled.[9] Because this technology can also support data (email, web, texting and instant messaging), it is cost effective for the telcos to bundle the data and voice on their networks under one technology approach.[10]

Consumers applaud better functionality at less cost and for the telcos, increased redundancy and fail over capabilities exist because the packet switched networks are able to use multiple paths to reach an endpoint. With this architectural approach, the telcos can now offer Internet based telephony (voice over internet protocol-VOIP) services to customers, where the phone numbers connect via gateway servers, which phone numbers are then tied to Internet protocol (IP) numbers.[11] Both PSTN and VOIP networks use databases to determine end-user locations. In order to complete a call, the two endpoints must be able to open and sustain a communication session.[12]

The features of a PSTN and a VOIP network are identical and to the user, often in-discernable. In both, oral communications and a direct connection exist that is sustained between the endpoints. Network telephony is not only cheaper but enables the user to get voicemail stored, printed and sent to multiple other devices for convenience. As such, one telephone call over a VOIP network can be tracked using any of the three Titles of the ECPA, based on the object law enforcement seeks. Tracking VOIP phone calls is critical to law enforcement. Skype, the leading VOIP provider had over 521 million users in the second quarter of 2010, more than most landline providers.[13]

Unlike telephone communication, email uses a "a transmission method by which a device receives a complete message or protocol data unit and temporarily stores it in a buffer before forwarding it toward the destination…" also known as 'store and forward.'[14] This feature of email is

important in the law as the third-party that temporarily stores the email message, likely the internet service provider (ISP), is now a part of the otherwise private transaction.[15] Typically, the ISP keeps a copy of the email message on its local server so that the end user can access it even after it's download to the user's endpoint device, laptop, handheld, etc. The fastest growing form of email is webmail, used by social networks such as Linkedin or Facebook. Social networking webmail had an estimated 820 million users in 2009.[16] And, an estimated total of 1.5 billion email users existed in 2009.[17]

The email use growth numbers reflect the transformation of how society now communicates. Google merged email with cell phone, home phone, SMS messaging and social media applications, all from a single handheld mobile device. The top telcos also drive this convergence and provide unified billing as major ISP's.[18] But unlike telephone which communication device requires continuous throughput of data, email has stop-points at which stop-point messages are copied and held (stored); this distinction remains a key test in the determination of how to treat privacy of communications under the ECPA.

As ubiquitous as email, instant messaging (IM) is estimated to have 2.5 billion registered accounts in 2009.[19] Like email, IM requires some software running on your device, most people use a browser from Firefox, Microsoft, Google or a mobile phone application. The IM provider maintains a server that the user logs into and then the user's device provides it with the port number (on your device), with which port number the IM server will communicate. The IM server then conveys to others in the user's group that the user is online and lets the user know who else is available to chat. Because each IM user provides port information to the server, any messages sent go straight through to the other IM user with no action by the server.[20] This instant communication, with its "XYZ is typing now," evidences the immediacy of the communication. The user is "talking" as fast as he can type and whoever houses the server automates all aspects of the communication. IM is akin to a fast email and with port connecting, almost like the telephone architecture. Monitoring an IM discussion as it occurs (in transit) or when it arrives (in storage) or just the port numbers used to connect the two endpoints (data attributes and connection information), again indicates three types of monitoring available under ECPA.

Finally, texting or simple message service (SMS) is the most prominent form of communication for Americans aged 13 to 34, with an estimated 857 billion SMS communications sent in 2008 and over 330 billion SMS messages sent in the first quarter of 2009.[21] SMS more closely tracks email with its ability to store and delay delivery of the message when the recipient is not ready to receive.[22] However, the use of the cell phone number and cell tower network combined with the immediate nature of the delivery if the phone is turned on, makes SMS a sort of hybrid of email and traditional telephony.[23] Based on the transfer and connect points for data in telephone, email, IM and SMS, the law divides what it can monitor at what point in a transmission.

These technologies both enrich and complicate people's lives. A flood of emails, text messages and phone calls occur throughout the day, covering all aspects of individual's lives from family

to work and school. All of these communication methods extend interpersonal relationships, from younger generations using texting to older generations sending Hallmark cards. In an American Bar Association (ABA) survey conducted on the use of technology among 5,000 members, the study revealed that 75% use smartphones (primarily to send and receive email) and 56% use Facebook or Linkedin.[24] The University of Colorado conducted a student use of technology survey, indicating that 90% of students use cell phones, laptops and university email daily and less than 10% use landlines.[25]

Since President Clinton signed the Electronic Signatures in Global and National Commerce Act "ESIGN" about 10 years ago, society embraced all things electronic. Under ESIGN, electronic signatures, contracts and records are valid and "may not be denied legal effect, validity or enforceability solely because it is in electronic form."[26] Where the same treatment exists for electronic forms of paper and actual paper, the question arises whether a different legal status should apply if that communication is sitting on a device in electronic form or has been printed out and placed in a file folder. For that matter, the privacy of a communication handed from person to person should be the same as when one's thoughts are reduced to a writing and communicated electronically. The U.S. mail does not open customer envelopes and similarly, the ISP contracting to deliver electronic mail makes a copy in transit solely to perform delivery, no inspection rights are granted by the sender.

Increasingly, law enforcement struggles with these new and emerging protocols to gain evidence against criminals or terrorists. Criminals like to fly under the radar and the sheer volume of communications across the network, combined with encryption from foreign source-points, creates difficulties for law enforcement to prevent the next terrorist attack. The correct balance remains in dispute, between openness in society and mechanisms to access data to protect Americans from highly motivated terrorists. Here, the technology outpaced the law but the threats are real. It is critical to preserve the capability of monitoring for law enforcement authorized under a warrant.

2. Defining the Borders of Privacy in Fourth Amendment Law

Americans expect privacy and courts recognize privacy in Americans' daily lives even though the U.S. Constitution does not explicitly use the term "privacy." The origin of any claim to privacy is the trespass area of tort law and extends privacy rights beyond physical interference to "the right to be let alone… and the term 'property' now comprises every form of possession -- intangible, as well as tangible."[27] "The principle which protects personal writings and any other productions of the intellect of or the emotions, is the right to privacy…"[28] This original understanding of privacy, derived over 100 years ago, could not have anticipated the digital age and difficulties in protecting written communications. This common law acceptance of a right to some privacy in one's daily life is bolstered by other fundamental principles of our rule of law.

The Fourth Amendment to the U.S. Constitution, for example, states "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall

issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[29] In 1700 it was simpler to determine if a person's papers were taken because "papers" meant actual paper. The only way to breach communications was to take the paper from a person or from a person's house. Landmark cases interpreted these words: "papers," "probable cause," and "particularity." These interpretations have direct bearing on the treatment of emerging forms of communications, even though the cases pre-date the technologies by 40 years.

Early caselaw, the basis for the modern communication statutes, addressed physical location and electronic communication. In 1960, the police attached a microphone listening device to the exterior of a home of a suspected gambler.[30] While the intrusion was minor, it was a violation of the Fourth Amendment because it was an "unauthorized physical intrusion."[31] The Fourth Amendment governs "not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any technical trespass under local property law under party walls."[32] Seven years later in *Katz v. United States*, a landmark case involving the government's listening to conversations conducted in a public phone booth, changed the law's view of telephone privacy, extending it beyond only those conversations intercepted following a physical intrusion.

Katz was convicted of wire fraud for transmitting wagering information using a telephone.[33] As evidence used to convict him, the government introduced information learned by the government from its listening to Katz's conversations using the phone in a public phone booth. The Court of Appeals agreed the government properly obtained the evidence because "there was no physical entrance" where Katz was talking.[34] The U.S. Supreme Court reversed, concluding that Katz was "entitled to assume that the words he utters into a mouthpiece will not be broadcast to the world." In other words, he had an expectation of privacy as a result, triggering the protection of the Fourth Amendment.[35]

The Fourth Amendment is not a general right to privacy under the Constitution. "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[36] The concurring opinion in *Katz* provides an informative perspective, proposing the following two-pronged test to determine if the expectation of privacy is reasonable:

"first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."[37]

Though the majority of the Court did not adopt this test, *Katz* firmly recognizes the existence of Fourth Amendment protections on people and their communications and in the light of what is reasonable both to the person and to society.[38] Today, with people sending email and text from the privacy of their homes to distant locations, whether those communications should still remain private is in large part based upon early telephone and physical mail delivery cases.

What is reasonable undergoes revision as society changes and must be based on the facts in each set of circumstances. To understand how courts assess reasonableness and may apply that concept in the future review of a sample of key cases is helpful. For example, providing information to a third party typically eliminates any reasonable expectation of privacy. A bank depositor had no rights in bank records seized, as such records constitute the business records of the bank, created at least in part from information voluntarily relinquished to the bank by the customer.[39] Similarly, if information is voluntarily given to the government by a third party, it is not protected by the Fourth Amendment.[40]

If control of information is maintained, then the court generally deems that information private and, therefore, applies the Fourth Amendment right to keep that information free from unwarranted government intrusion.[41] However, financial records voluntarily handed to a financial advisor and then given to the IRS by that advisor does not trigger the Fourth Amendment, as providing the information to the third party relinquished control of its privacy.[42] Similarly, when a person neglected to pay for a locker, he lost his rights to the locker contents and the government could use the contents (computer tapes) as evidence against him.[43] This approach is somewhat like a bailment, where the person's rights are preserved as long as the bailment contract is in effect but are extinguished when he fails to re-claim his property (abandons it) or neglects to pay his fee (as here). The government justifiably seized the information because bailor no longer had a Fourth Amendment right to protect to the contents of his package.

In the realm of written communication, sending a letter through the mail ensures privacy of the inside of the envelope while en-route but the receiver then decides whether to keep the message private. Where the husband-inmate sent letters to his wife from prison, which letters were later used against him as evidence, the court said that the expectation of privacy in the contents of the letters terminated upon delivery to his wife.[44] While paper communications and package contents are private while being transferred from sender to receiver, the court typically finds that private carriers such as Federal Express, can gain access to private contents through the stated terms of the service contract.[45] Through consent, the shipper can eliminate his privacy rights in letters and packages in the hands of the common carriers. Absent consent, there is an expectation of privacy during carriage, but also the risk the carrier will deny carriage without such consent.

People regularly give consent for access to medical, financial and other types of personal data in order to get credit, apply for jobs, to buy a home and once done, that consent travels from the recipient to third parties, unless there is some prohibition elsewhere in the law.[46] Information requests are stratified, as some data can be shared while other

cannot. Even though legislation established privacy in bank accounts and medical data, the core principle that giving information to a third party enables it to be shared with others, is now part of the federal government's information sharing initiative.[47] Moreover, intangible information can also be "seized" by interception and if done by a private individual, outside the direction of a government agent, there is no Fourth Amendment protection.[48]

In more recent Fourth Amendment cases, the court clearly struggled with technology advancements. To track a suspect, a Drug Enforcement Administration (DEA) agent placed a beeper monitor into a can of ether and replaced one of the informant's cans to be delivered to the suspect's car.[49] The suspect brought the can into his home and the DEA monitored the beeper and ether shipment inside his home.[50] The issue was whether the DEA beeper monitor violated the Fourth Amendment. The Supreme Court ruled that the beeper was reasonable when placed in the car, and unreasonable when it entered the home.[51] Privacy issues are strongest when the object is in the home and become weaker as the object moves just outside the home and finally into a public area.

In another close call, the police used a thermal imaging device to capture heat emanating from a house, to prove the target was growing marijuana.[52] "[t]he Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant."[53] In enforcing the warrant, Justice Scalia noted thermal imaging was a new technology, not in general use.[54] This suggests that the Court is mindful of technology's ability to displace traditional boundaries, such as inside versus outside.

Then, as now, the telephone required a warrant for the ability to listen in on a person's phone call.[55] The warrant requires probable cause and must be issued by a detached, neutral magistrate.[56] Evidence collected by listening devices, without a proper warrant issued in advance, is excluded from the record in courts.[57] However, evidence is not excluded based on police error if they "acted on objectively reasonable reliance on the subsequently invalidated search warrant."[58] Excluding evidence based on administrative error was not going to deter police misconduct. "Police conduct must be sufficiently deliberate that exclusion can meaningfully deter it."[59] However, the dissent in *Herring v. United States* expressed concern that databases form the "central nervous system of contemporary criminal justice operations and span the terrorist watch lists, National Crime Information Center (NCIC), purchased commercial databases and are often out of date or inaccurate."[60] The opportunity for abuse is real, if evidence of wire or electronic communications is admitted into court under this lesser standard. Moreover, it will be hard to demonstrate law enforcement is not acting reasonably as new technologies develop keeping technology always one step ahead of the law the officers are applying.

People typically think of the Fourth Amendment right to privacy in the content of communications. In 1979, the police collected the phone numbers dialed from a "pen register" and used that evidence against a criminal without having first obtained a warrant.[61] In *Smith v. Maryland*, the Court found that Smith had no expectation of privacy in the

phone numbers he provided to the telco. The telco recorded the numbers for business purposes, thereby removing any Fourth Amendment need for a warrant, for the government to obtain those numbers from the telco.[62] The petitioner likely had a privacy expectation in the content of his communication by telephone, but that was not at issue.[63] Content, what is said or heard or written to convey an idea, is more important than the delivery mechanism and the related attributes, such as: phone numbers, an address on the outside of envelope, an Internet IP address, an email recipient address or a web URL.[64] The courts adapt physical world situations to intangibles to incorporate new technology. Like the law, technology also changes both incrementally (wired telephones to wireless, to voice over IP) and into entirely new areas (Internet email, web searching, texting and peer to peer communications).

The challenge for legislators and the courts is discerning 'like' or dissimilar technology. Content v. non-content is a good benchmark but it's not all-inclusive. Our statutes overlay Internet based communications onto telephone technology but modern communications are more sophisticated and what was simply connection information for telephones, is richer data when monitoring the Internet.

3. The Electronic Communication Privacy Act (ECPA)

In 1986 the U.S. Congress passed the ECPA to add protection to an emerging electronic marketplace, primarily computers and bulletin board systems. The goal of the legislation was to treat electronic mail and web message postings with the same privacy afforded telephone communications.[65] The early use of electronic communications formulated legislation that followed the then-current usage. For example, bulletin boards are effectively an open notice newspaper listing and should not afford much, if any, privacy.[66] Early email however, was seen as more akin to U.S. Mail and should receive the protection of an un-opened parcel, containing content.[67] Yet, that protection vanishes when the U.S. mail reaches the sender and it becomes the decision of the recipient to keep the contents private or not.[68]

Email includes content that is necessarily exposed to the ISP transmitter. The legislators attempted to keep the email as private as telephone communications for what seemed a reasonable time frame (six months) and thereafter, the email is degraded in its status.[69] One explanation for treating old email with less protection might be the cost of memory for storage of email and other data.
In 1986, the cost of three megabytes of memory was $568. The cost for memory in 2009 was approximately $45 for 4 gigabytes. Some quick math indicates that the cost in 2009 is 1/11th that of 1986 and the buyer receives 1300 times as much memory![70] Storing email in 1986 was expensive and it was reasonable to expect that there would be few emails stored after six months.

If you consider the terabytes of data storage that are common today and the lay person's ignorance of the law, much email now falls under lesser protection because it is stored for a year or longer. The object, the location and the time or duration for the communication in storage enables law enforcement to compel discovery by matching those criteria to requirements for a subpoena, a court order or a warrant.

Congress significantly amended the ECPA with the Communications Assistance to Law Enforcement Act (CALEA),[71] the USA-PATRIOT ACT in 2001, the USA-PATRIOT reauthorization acts in 2006, and the FISA Amendments Act of 2008.[72] This paper reflects those amendments but will highlight only certain legal changes key to the discussion.

The ECPA is broken into three sections, each addressing a communication in transit, storage or the connection data that is incidental to that communication. Title I is the federal Wiretap Act under 18 USCS §§ 2510-2522 covering wire, oral and electronic communications in transit. Title II is the Stored Communications Act (SCA) under 18 USCS §§ 2701-2712, covering electronic communications in storage. Title III is pen register/trap and trace statutes 18 USCS §§ 3121-3127, covering dial, routing, addressing and signaling information.

At a high level, the strongest protections are afforded the oral communications in transit and the least are connection information or non-content, connection information. The three sections of the statute are intertwined and the SCA uses definitions from the Wiretap Act. Also, the content portion of a protected communication under SCA will see its routing information lesser protected under the trap and trace statutes. For this reason, its important to look at all three sections, as the same electronic communication receives different treatment based on where it is in its life cycle and what portion is sought by law enforcement.

4. The Stored Communications Act

The SCA is a criminal statute that affords protection to unlawful access to electronic communications.[73] When Congress drafted the SCA, it categorized two types of entities that would process information, an electronic communication service (ECS) and a remote computer service (RCS).[74] The ECS, means any service, that provides to users thereof the ability to send or receive wire or electronic communications.[75] "A communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire)."[76] The RCS, means the provision to the public of computer storage or processing services by means of an electronic communications system.[77] An easy way to think of this distinction is, an ECS is paid to send and receive email, if a person has a lot of electronic files that they want to keep safe (disaster recovery, back up), then he would pay an RCS to perform that storage function.

Generally, a telco or an ISP is considered an ECS but private companies can also get that designation. Examples include Netscape providing email services or AOL providing bulletin board services or even email offered by an insurance company to its agents.[78] In defining the parameters of an ECS, the court held that access to text messages was warranted by an exclusion with the SCA..[79] In effect, your employer (as an ECS) has access to employee communications and this network access to services is typically augmented by some formal consent in employment agreements.[80] If the service does not enable a person to send or receive a particular communication, it doesn't qualify as an ECS.[81]

This definition extends to cover businesses like eBay that sell goods online but don't enable messaging directly between parties. Ebay is not an

ECS because they use other ECS services.[82] Consider that the user's ISP will be the first ECS subject to the SCA and the users's employer or university providing network access might be the second. Both entities have rights to examine content either in the ordinary course of business or because the user has consented in a network access provisioning agreement. Last, if the ECS is not a generally offered "public service" then they can volunteer the information to the government without a warrant or a court order.[83]

The RCS seems straightforward as an ability to store electronic files with a third party. Today, many services offer remote storage at low fees and Google even offers up to one gigabyte of non-google docs for free.[84] The lines blur a bit because while companies such as Google offer plain vanilla storage, they also offer a public email service, qualifying them as an ECS. The SCA approaches this blurring by designating the communication as the trigger to what statutory jurisdiction applies. Thus, if the communication is in transit, the federal Wiretap Act applies,[85] but as soon as that communication goes into storage by the same ECS provider, that communication (email, etc.) is then covered by the SCA. The definition of electronic storage includes:

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.[86]

From the above definition, imagine that an email is sent through an ISP. The message is held while a copy is made and simultaneously sent to the ISP of the recipient (where another copy is made) and finally the recipient's mailbox requests its copy of the email message. Two opportunities exist for copies and temporary storage to occur, both with the ISP acting as ECS and with the recipient ISP.

When the user opens an email he is given the option of deleting that message from the ISP's server. If he chooses not to delete it from the ISP server, then that message that was opened and read by the recipient, is now "in storage" by the ECS. This distinction has produced a split in the U.S. Circuit Courts of Appeal, as to whether the email converted the ISP from an ECS into an RCS as soon as it stored the email.

If the message is in storage by an ECS as opposed to an RCS, it is harder for law enforcement to gain access to the content. The content includes the files and the meaning of what we intend to communicate. "[w]hen used with respect to any wire, oral, or electronic communication, [content] includes any information concerning the substance, purport, or meaning of that communication."[87] Certainly, this is the most important aspect of the communication. But there is also connection data, IP addresses and session data, that is ancillary to the content and not subject to the same protections as content.

Connection data only requires a court order as opposed to a warrant.[88] Email has both content and non-content information. The courts examine how the communication occurred, where it was intercepted, how the government has accessed the content and whether there was an expectation of privacy in that communication.

5. Law Enforcement Tools to Compel Disclosure under the ECPA

A government entity may require an ECS or an RCS to provide data using different mechanisms. Basic subscriber information can be obtained under a court order or administrative subpoena, including: name, address, telephone number, records of session times and durations, length and types of service, IP addresses and means of payment, including credit card numbers.[89] The subpoena can also be used to capture information that falls outside of the ECPA. This reflects the low bar of access to data.

Law enforcement may also seek records that may be more instructive than non-content but not as revealing as content, for example, subscriber or customer information. In this case, the law requires prior notice and a subpoena.[90] Using the prior notice combined with the subpoena can also secure content held by an RCS and content held more than 180 days by an ECS.[91]

In order to gain access to content, the government must indicate whether the content is held by an ECS or an RCS. If it is held by an ECS and the content has been stored for 180 days or less, a warrant is required. If the content has been in storage for more than 180 days, then the same rules that apply to an RCS go into effect.[92] Here the time element transforms 'super protected' data to 'lesser protected.'

After email is held for180 days, prior notice combined with an administrative subpoena or a court order, will suffice.[93] This reduced protection for longer stored communications is a lesser burden on law enforcement, presumably because the long-term storage of the contents imply less value and, thus, presumably a lessened expectation of privacy.

If the government wants to collect account log data, it must comply with § 2703(d), under a court order from a federal, state or district court judge. This approach can collect all opened email held for less than 180 days if combined with prior notice or delayed notice (up to 90 days), if they can show that notice to the subscriber would case harm or damage evidence.[94] The delayed notice is logical because you don't want to lose access to evidence by tipping off the target but the lack of notice is problematic if unchecked.

Finally, if the government obtains a search warrant under Rule 41 of the Federal Rules of Criminal Procedure, it can collect all non content information, account log information and customer information using the lesser standards above as well as all content contained in the subscriber account.[95] The warrant is the most powerful tool in collecting all types of data (content and non-content) but it is the most difficult to obtain. Law enforcement applies the statutes to collect evidence against criminals and terrorists but the definition in the statute do not always match up with the traffic seized.

6. The Courts Fight over Email Obtained through Law Enforcement

If the ECS is a public service, it cannot voluntarily offer information to the government. If the ECS is a private company or university or some entity that is more interested in providing itself with a service, then it can provide information without warrant or subpoena.[96] With the tiered compelled disclosure rules set forth above, the government can proceed to collect evidence of criminal or terrorist activity but the courts continue to look to the common law and the U.S. Constitution in addition to the letter of the statute. If law enforcement suspects a person is planning to bomb a location and they get a court order to read all text and email messages going

to a certain person, they may invade the privacy of innocent persons but that is something that society recognizes as reasonable.

Effective prevention of terrorism must be swiftly executed. The public expects government to listen to law enforcement even where a certain percentage of court ordered warrants will turn out to be a false alarm. In 2006 when news broke of NSA surveillance of telephone lines, a survey showed that 63% felt it was justified to keep America safe.[97] The courts will strive to find a balance between protecting Americans from terrorists and eroding personal privacy from unfettered government monitoring.

Telephone monitoring is more easily understood to Americans and the courts than generic network monitoring. This lack of understanding is problematic given the split in the U.S. Circuit Courts. In the *Theofel v. Farey-Jones* decision in the Ninth Circuit in 2004, a private party was abusing the subpoena power to collect email from a litigant.[98] Defendant Farey-Jones sought all of Plaintiff's email from his ISP Netgate, without any time or scope limitation. The Plaintiff enacted a civil suit for violation of the Wiretap Act and the SCA and the District Court held that the statutes did not apply.[99] On appeal, the court applied the common law of trespass.[100] The defendant's position, was that previously opened emails, were not in electronic storage and thereby, not subject to the protections of the SCA.[101] However, the *Theofel* court determined that the § 2510(17)(B) back-up provision applied and the ECS label was proper.[102]

The SCA covers temporary back up storage incident to the communication or back up copies. Yet several cases had interpreted storage to mean that once the emails were opened by the recipient, they were no longer in electronic storage.[103]

It seems logical as an email user, that if the user deletes his email from his smartphone, when he turns on his Macbook, he may still want to download and read that same email already opened on a different device. He is using the ISP server as a back-up for his email access and the Court pointed out that the SCA does not require the back-up be for the ISP. This approach to analyzing the storage of emails was thought to provide greater protection to users of large ISP's based in the Ninth Circuit, such as Yahoo and Microsoft Hotmail.

But in 2009, the Seventh Circuit distinguished *Theofel* and allowed the government access with a trial subpoena instead of a warrant, to 'web-based' mail held less than 180 days and previously opened.[104] Even though Microsoft was physically located in the Ninth Circuit, the Seventh Circuit trial subpoena was enforceable nationwide.[105] Access was appropriate under § 2703(b)(2) and not still covered by the ECS storage under § 2510(17).[106]

An argument exists that only while the email is unopened, is it is still in electronic storage.[107] The Third Circuit agrees and adds that after it has been received, the temporary and intermediate storage (of email) are completed and no storage is incident to that communication.[108] In Pennsylvania, the DEA read opened emails pursuant to the SCA and did not need to provide notice to the subscriber and the government agents and attorneys had full immunity from prosecution in civil claims.[109] Any of the Circuits are available to a government prosecutor if the ISP or the communication is stored within that district and court ruling is enforceable nationwide.[110]

Yet in another circuit, the court focused on Congressional intent and plain language of the relevant statute.[111] Additionally, the Sixth Circuit, agreed with *Theofel* and concluded, "The fact that Plaintiff may have already read the emails and messages copied by Defendant does not take them out of the purview of the Stored Communications Act.".[112] In the Circuits where the *Theofel* line of cases continues to hold, the government must treat all emails held by an ISP as an electronic communication regardless of whether the recipient has opened the email.

The courts examine the Wiretap Act and the SCA provisions on each communication in an effort to address the 'in transit' or 'in storage' transmission dichotomy. Yet, different conclusions continue among circuits … It's instructive to take a closer look at the way law enforcement uses the Wiretap Act to compel email and other network protocols (text, etc.).

7. The Wiretap Act as Related to Email

The Wiretap Act primarily focuses on providing a balance between the need to protect citizens from unapproved wiretaps from the police but enabling law enforcement to collect evidence on criminal activity.[113] When the ECPA passed in 1986, it included electronic communications in addition to wire and oral communications. The Wiretap Act focuses on intercepting and in order to intercept something, it must be in transit.[114] In contrast, the SCA is focused on data at rest or in storage.

A wire communication is an aural communication, handled by an ECS, that includes the human voice.[115] Or, it includes an "oral" communication, that denotes an expectation of privacy by the person talking and specifically excludes an electronic communication, such as an email.[116] This statutory definition includes VOIP communications from Vonage, Skype and others, that utilize the network to deliver oral communications.

When a wiretap is requested, "the application for the order must show probable cause to believe that the interception will reveal evidence of a predicate felony offense listed in § 2516."[117] Any evidence collected that does not comply with the statute under §§2510-2520, is inadmissible in court.[118] However, under § 2707 of the SCA, exclusion of evidence is not a remedy.[119]

Essentially, its more difficult to gain access to data protected by the Wiretap Act and if you don't follow the statute, you lose the evidence. Whereas, the SCA has weaker protections for its data and even if the police improperly obtain data, they can still use the evidence in court to prosecute the defendant.

In today's networked environment, law enforcement faces immense challenges when attempting to catch a criminal or a terrorist. The aggressive nature of the criminals encourages law enforcement to be creative within the rules. In one instance, the FBI installed a key logger onto a computer to capture a password and they configured the device to operate only while the modem was turned off, thereby not triggering the test of recording 'contemporaneous' with transmission.[120]

The police are able to insert themselves as a "man in the middle" and monitor your email as it crosses a network, but as the cases show, there is disagreement as to whether this action is an intercept or a seizure of stored data. A book dealer read emails as they transited the network and claimed that they were in storage and not subject to the Wiretap Act.[121] The court disagreed and stated that while it was not an interception using equipment, the email was in

transient storage and a part of the transmission therefore the government intercepted it in transit.[122] Software is readily available to read email in transit before it even gets into temporary storage.[123] In other Circuits, that same activity by law enforcement would not be interception because of the view of 'what is stored.'

In a related ruling, an ISP terminated the account of what it thought was a spammer and continued to receive that person's email and store it. When the ISP concluded that its customer was not a spammer, they re-instated his account and forwarded all mails collected to the customer.[124] The ISP was acting in the ordinary course of business and did not intercept the email.[125] This result is fair because the ISP did not intentionally collect and review the customer's email and spamming is a big problem for ISP's and customers.

This case shows how civil liability is an appropriate way to resolve such an issue but it does raise concerns. An ISP should delete all emails when an account is terminated [126] The government should be denied access to all email and connection data for accounts as they terminate with an ISP, even if the objective is to perform data analysis to capture terrorists or for information sharing. All ECS and RCS companies should delete all data when a relationship terminates and not share that data with any third parties.

8. Trap and Trace Statutes Applied to Internet Communications

The third area of the ECPA is the Trap and Trace statutes under 18 U.S.C. §§ 3121-3127, that focus on non-content information.[127] With an application to the court, the police may place a device on an ISP network and record all IP address information for a particular customer, log data, to and from information in email messages and connection data.[128] It is widely believed that this information is not as valuable as content and should be subject to less privacy because the user exposes it to access or deliver the content, both in web searching and email transmission. In 1995, the thinking was that tone devices fell within the electronic communications of the SCA but that trap and trace devices were primarily for telephones.[129]

Users now have many new types of revealing data from Internet traffic and it can be collected by a trap/trace device placed at an telco/ISP. Web pages are descriptive and URL's will lead a user to a specific document with full text. An email address will define an individual, whereas a landline phone number will only define a house. If the search string in a web browser exposes content, that search query entered would reveal a person's thoughts.[130] If the search results returned include content, the same invasive result occurs.

What was originally authority to track a telephone number blossomed into a treasure trove of location information and content, all shown by an IP address or web URL. Yet law enforcement has its best chance at capturing terrorists by collecting this seeming innocuous data because it not only tells about the target but with whom they are connecting online.

In 2009, there were a total of 1764 authorized wiretaps (wire, oral and electronic communications) and each order had an average of 688 incriminating intercepts.[131] That's a total of 684,000 incriminating pieces of data. To suggest that there is not value in wiretapping to help prevent terrorism would be foolish. But the connection data

that is helping to capture terrorists presents different issues, such as what innocent person's data is collected alongside a target or what content is naturally a part of the non-content (a web URL).

In an attempt to show that the search engines return information on child pornography, the government sought to include the major search engine providers in compelled discovery.[132] Google objected to the government's request for production and the court agreed that providing a million query results was excessive as was the full text of 5,000 queries and a compromise was reached.[133] The government's request of Google indicates that the results alone from a web search yield valuable information and trademark protected property (algorithms), even if its just URL results. The ability to gain significantly more information from these uses of trap and trace type devices demands some consideration of the proper balance between government and individual interests.

9. The Courts Balance Competing Interests

When the police are tracking a terrorist, they look for the data at the known residence, workplace, telco/ISP, associates locations and increasingly the Internet.[134] If law enforcement picks up a transmission from a trap and trace and want to follow it back to a source, it could lead to an ISP, a home or a workplace. In addition to analyzing what type of transmission it is, where the data resides will determine what action the police can take. If the data resides at the workplace, the user has a reasonable expectation of privacy in the contents of their computer at work, if it's a private computer and not for general use.[135]

It's important to balance "the nature and quality of intrusion on the employee's Fourth Amendment interests against the governmental interests alleged to justify the intrusion."[136] The Court talked about the operational realities of the workplace and stated, "we must balance the employee's legitimate expectations of privacy against the government's need for supervision, control and the efficient operation of the workplace."[137] Even though there was no warrant or probable cause, the Court found that there was no need to reach a Fourth Amendment question because of the need for balancing competing interests.[138] This confirms that the courts will closely follow the facts of each case and narrowly interpret the Fourth Amendment.

Where an employee had child porn on his computer, the court found a subjective expectation of privacy in a workplace computer but not an objective expectation, particularly where the employer consented to the search and the computer remained a workplace property.[139] In a case involving wire fraud, the government used the § 2703(d) delayed notice provision when it got the courts permission to read email for over a year.[140] When the petitioner challenged the constitutionality of the governments' actions, the appeals court decided that the action was not fit for judicial review because "they didn't know if the government would search his email in the future and he already had notice that they had searched his email and presumably could again, but could not know the specifics of his email service provider and how this might occur."[141] This result shows how the lengths to which courts will go to avoid a constitutional question, particularly in such new and ever-changing areas, and in the process, the petitioner may be frustrated.

Similar cases emerged where the data is not at the workplace when law enforcement accesses it

but is at the ISP. In one instance, the government placed a device at the ISP to monitor all of the IP addresses and 'To/From' information for all email for the defendant.[142] The Ninth Circuit stated that this was a case of first impression but they felt that it fit comfortably within the Pen Register statute of non-content and no Fourth Amendment violation occurred and suppression of evidence was not a remedy under the statute.[143]

In a case involving stolen customer lists, an employer used passwords that were left on company property to access email accounts and their contents held at webmail providers Hotmail, Gmail and a private company.[144] The court concluded that the employer was never given access to those accounts even if they could show that he had accessed the remote accounts while at work.[145] The employer had violated the SCA because even if the employee had consented to all network access, the employer did not own these remote webmail services. The court also stated that the petitioner had a reasonable expectation of privacy in the email.[146] If an employer suspected that his current or former employee was a terrorist, monitored email and turned over the records to the FBI, with the SCA as the operating statute, the evidence could not be suppressed even though it was improperly gathered.

In 2008, the Ninth Circuit decided that a text service used by the City of Ontario police department was provided by an ECS and not an RCS.[147] The Defendant ISP attempted to use the 'store and forward' label as excluding the text service from an ECS environment but that argument was dismissed because SMS is commonly known for communicating as compared to document storage offerings.[148] There was no RCS storage or processing service being provided to the city.[149]

In order to reach the Fourth Amendment privacy question, a 'balancing of interests' test is applied.[150] "The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question…do the users of text messaging services have a reasonable expectation of privacy in their text messages stored on the provider's network? We hold that they do."[151]

Even though there was a formal written network policy in place covering privacy on the city networks, the supervisor overrode it with a verbal policy.[152] It is a close call but there was a history of reliance on the verbal policy and for that reason, the court didn't enforce the agreed-to network policy. The City of Ontario violated his reasonable expectation of privacy because there were less intrusive methods to determine if he had exceeded the allotted 25,000 characters.[153]

In 2010, the U.S. Supreme Court reversed the Ninth Circuit in *City of Ontario v. Quon*, concluding that the City of Ontario was motivated by a legitimate work related purpose and the search was not excessively intrusive in light of that justification.[154] Quon's Fourth Amendment rights had not been violated because a standard of reasonableness should be applied under all the circumstances.[155] Even if Quon had a reasonable privacy expectation in his text messages the company's interests were greater.[156]

The Court ruled that reading the SMS messages was a search in the electronic sphere and has characterized SMS for future law enforcement actions.[157] SMS is an ECS function and text

messages shall be treated to the more stringent warrant standard under the 180 day rule for messages held on the network or if intercepted in transit.

City of Ontario decided important issues for the workplace but they will have impact on law enforcement, as the FBI needs to track SMS for criminals and terrorists. Gaining access to SMS messages will be as difficult as getting authorization for a telephone wiretap but Congress' amendments to the USA-Patriot Act and FISA provides alternatives.

10. The Impact of the USA Patriot Act and FISA on Network Communications

September 11th is now a part of U.S. citizens' shared history as Americans, and this last decade forced issues to the fore that are difficult to reconcile. The world is digital; personal identities, communications and website properties, are all scrutinized as part of the war on terror. This non-traditional war requires that Americans protect themselves and their data. Online blueprints to a nuclear power plant could result in a "real world" attack if terrorists are able to access that public or private website. Often terrorists plan and prepare for such physical attacks online, using encrypted communications.

VOIP programs such as Skype are widely used and the encryption is automatic and quite strong. Skype also employs scrambling of ports making it difficult for network operators to know where Skype is entering or exiting a network, if tasked by law enforcement to track communications.[158] This type of protocol is called "peer to peer" or P2P and became popular with Napster and music downloads.

P2P is growing as a percent of network usage for movies, music, video and online communication. Terrorists can use Skype too. Unfortunately, the telcos may not even know the amount of Skype traffic on their network unless they are using deep packet inspection to track network content.[159] Skype provides a technical challenge to law enforcement. In response, Congress passed CALEA in 1994.[160] CALEA covers all common carriers, broadband providers and VOIP providers. It mandates that they procure enabling technology that law enforcement can use to access and read content to telephone, email, voicemail and now, encrypted communications.[161] Costs for compliance are to be borne by the provider and if the provider chooses to outsource to a third party, the obligation is not lost.[162] The government is relying on the telcos and the ISP's to better enable enforcement of the statutes.

A court ordered warrant must be enforced but it should not be at the expense of a third party. Recent reports suggest that the telco architectures must be designed or re-designed to address this government need.[163] This redesign effort could prove costly and time consuming and may interrupt or degrade the telco service. This new effort may also call for software vendors to put in a "back door" so that law enforcement can access and decrypt communications.[164] Years ago there was talk of putting a "V-Chip" into all network boards similar to technology used to control televisions but that never happened.[165]

In today's environment of terrorism, that initiative may get a similar response to the CALEA initiatives. The difference between CALEA and the V-Chip, is that the monitoring or decrypting of personal communications would be happening at the third party carrier location, not in the home on a private computer. In addition to CALEA, the USA-

Patriot Act broadened law enforcement access to communications.

The USA-Patriot Act passed in 2001, shortly after the 9/11 attack.[166] The USA-Patriot Act updates many existing statutes beyond the ECPA, but within the wiretap arena significant changes exist that affect law enforcement. Specifically, Title II Enhanced Surveillance Procedures, covers both ECPA and FISA modifications.

The USA-Patriot Act largely addresses terrorist threats, believed to originate overseas. For domestic crimes with foreign agents or participants, the FISA statute has emerged as a powerful tool of law enforcement.[167] FISA is focused on foreign agents and the collection of intelligence data to catch a terrorist operating in the United States.[168] Electronic surveillance under FISA anticipates a future event whereas a warrant is issued under the ECPA when there is evidence of a crime committed.[169] But providing too much power to the executive branch for monitoring in the technology area combined with secrecy of the national security letters, can disrupt the checks and balances of our government.

FISA is different from the ECPA in that it doesn't require that the target be involved in a crime;[170] there is no notice provision;[171] it requires the nature and location of the facilities and the type communication, not the particularity of the things to be seized;[172] and the place surveilled doesn't have to be connected to the crime.[173]

In addition, key changes to the ECPA and FISA from the 2008 USA-Patriot Act include: the government can request surveillance authorization for terrorist activity;[174] roving wiretaps are issued under FISA;[175] FISA wiretap initial periods expanded from 90 to 120 days and extensions increased from 90 days to one year;[176] voicemail messages are compelled under the less stringent SCA rules with no evidentiary exclusion;[177] subpoena powers to compel subscriber information now include Internet IP addresses and credit card information;[178] approval for FBI use of delayed notice "sneak and peak" warrants;[179] and Pen Register use against U.S. citizens under FISA.[180]

Perhaps one of the most important updates made to FISA from the Patriot Act, is the change from "the purpose" to "a significant purpose" in the application made to the FISA court.[181] If the primary purpose was for domestic criminal prosecution but a significant purpose was the collection of foreign intelligence, then FISA can now be used against an American.[182] "Whether Congress's disapproval of the primary purpose test is consistent with the Fourth Amendment - has no definitive jurisprudential answer."[183] While the FISA surveillance may not meet the probable cause standard, the surveillances it authorizes are constitutionally reasonable.[184]

Two concerns emerge, i) that evidence collection may not be approved under the more stringent warrant test and ii) evidence under FISA will not be excluded if found to be improperly collected. The "programmatic purpose to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from ordinary crime control."[185] The government's expanded access could cause more issues to arise as to the proper statutory application and handling of new technologies by the courts and the other branches of the government.

In 2009, the FBI made 1329 applications to the FISC for electronic surveillance and eight were withdrawn and one was rejected.[186] The same report

noted that the FBI made 14,788 National Security Letter (NSL) requests in 2009. The NSL is an administrative subpoena issued by a government agency to compel disclosure applicable to electronic communications.[187] While the NSL can be challenged in court, it will likely be complied with by the recipient (ISP or other). This speeds the process for the government and may give access to data that would not be given if the government had to seek a court order. Once all of this data is collected via FISA or NSL and made available to other agencies through information sharing, the concern for individual privacy escalates because this data can be used in criminal prosecution.[188] "We must be vigilant over who makes the decision [to issue a warrant] and that the President and Attorney General can never be a disinterested magistrate, not even for matters of national security."[189]

In 2007, the government charged a U.S. citizen with participation in the Madrid Spain train bombings based on FISA information.[190] The investigation leading to the arrest and the arrest itself were the result of a false fingerprint match, leading the FBI to file an application with FISC to conduct electronic surveillance on Brandon Mayfield's home and office.[191] Mayfield claimed that FISA undermined the requirements of probable cause "as a precondition for obtaining a search warrant and for collecting, retaining and disseminating the information thus obtained."[192] He added that FISA violated the Fourth Amendment by permitting warrants without showing the primary purpose to be that of foreign intelligence information.[193]

On appeal, the Ninth Circuit decided that Mayfield did have ongoing injuries from the government retaining information it had collected. But the court held that the Declaratory Judgment would not redress that injury and the plaintiff had no standing for the Fourth Amendment claim.[194] While Mayfield lost the Fourth Amendment claim on procedural grounds, the court did not reverse their holding of the unconstitutionality of a search conducted under the "significant purpose" modification to 50 U.S.C. §§ 1804 and 1823 under the Patriot Act Sec. 218.

Since the Patriot Act amendments to FISA, all but one court supports the 'significant purpose' as opposed to the pre-amendment language 'primary purpose', but cautioned that if the sole purpose were criminal or no foreign intelligence was sought, the outcome would likely be different.[195] "It was our intent when we included the plain language of Section 218 of the USA- PATRIOT Act and when we voted for the Act as a whole to change FISA to allow a foreign intelligence surveillance warrant to be obtained when "a significant" purpose of the surveillance was to gather foreign intelligence, even when the primary purpose of the surveillance was the gathering of criminal evidence."[196]

11. Current Challenges to finding the Correct Balance

The law struggles to keep up with technology but it cannot ignore the implications of how communication networks changed and continue to change and the resulting impact on privacy in daily communications. Email, texting, instant messaging and voice over IP are dominant forms of communication, can share multiple copies of the same communication in near real-time and are overtaking the telephone. The protections afforded telephone communications should be extended to include these emerging forms of communication.

The fact that an email or text message is stored for six months or two years, should not lessen the privacy of that data. It remains a personal thought, it could be a copyrighted piece or some form of intellectual property with rights asserted. An ISP cannot gain property rights in a private communication as the intermediary performing a service. "Privacy is not a discrete commodity, possessed absolutely or not at all."[197] The notion that we assume the risk of disclosure by sharing non-content data, presumes we have made some choice. But with telcos and ISP's, the user has no choice if he wants to use a cellphone or a computer on the Internet. The only option for the user is to encrypt his communications to ensure integrity of the data, even that will not protect against forfeiting basic connection data.

The telco/ISP should offer the consumer the same high level of privacy that it provides to its corporate customers under master service level agreements.[198] At a minimum, users should know if their email or text messages are being seized under a warrant at completion of the surveillance. Yet, *In Re U.S.*, held that the USA-Patriot Act amendments to the SCA 2703(a) included the procedural but not substantive elements of the Federal Rules of Criminal Procedure 41, meaning notice to the subscriber can be suspended or never provided.[199] The lower court held notice of the warrant served for content of email had to go to the email subscriber. On review, the District Court determined that notice to the ECS (the ISP) was sufficient.[200]

In Re concluded that the government wasn't "taking property" so it wasn't a violation.[201] "Much of the reluctance to apply traditional notions of third party disclosure to the e-mail context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our e-mails. Some people seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not."[202]

Paying for a carrier to deliver your electronic mail is different than leaving papers at a friend's house, which papers are then subject to a warrant served on the property.[203] If the intangible property (email) is used as evidence, it is no different than a gun from a crime scene or a DNA gene sequence patent filing.[204] When law enforcement reads or views private electronic communication (handles it), it is a seizure of the essence of that information and the subscriber/owner of that intangible property should be put on notice.[205] These new forms of communication are a necessity if a person is to function properly in society.

If Congress amends the statutes to treat the content of new communication protocols with the same propriety as a telephone wiretap (warrant required for access), it would restore the Fourth Amendment protections as the initial court cases were decided in the 1960's. Society has embraced the digital world and Americans electronic property is scattered across many geographically disperse locations but protections are weak outside the physical home.

The data attributes which surround content and bring it to a specific endpoint, as well as web queries and results, should also receive greater protection. Recent attempts by law enforcement to capture geo-location data for real time tracking of cell phones, threatens Americans' privacy of movement. The government's position is to combine the Pen Statute, CALEA and SCA and imply a right

from the aggregate statutes to gather cell site tower information.[206]

Consider that the Pen Statute allows law enforcement to get access to non-content and signaling data (cell site location) with a prospective order.[207] CALEA enables access to cell site location from a court order.[208] SCA requires the probable cause standard of specific and articulable facts showing reasonable grounds to get historical cell site information.[209] Law enforcement wants real time cell phone tracking under a lesser standard than the SCA. The government claims the combined powers of the statutes are sufficient because the words "soley pursuant" in CALEA indicates Congress' intent to combine the SCA and the Pen Trap statutes resulting in a hybrid order.[210] Several courts have rejected this hybrid approach and two have allowed it.[211]

This problem is complex because cell phones can functionally operate as beepers or tracking devices although their primary purpose is to convey private communication. If Congress wants law enforcement to have this tracking capability, they could amend the ECPA. No citizen wants their movements to be tracked and traced throughout the day. The government does not currently collect all of this non-content data but it purchases data annually and performs data mining.[212] An erosion in personal privacy will accelerate if cell phones are included by law enforcement to show location data without a warrant because as currently drafted, the statutes treat non-content data as unimportant.[213]

Last, the war on terror and the use of FISA surveillance orders on U.S. citizens is alarming. Most Americans want to catch criminals (domestic) and terrorists (primarily foreign) by following the rules enforced by the courts. Consider a domestic criminal in the import/export business who is part of a crime ring and as a result, his communications go overseas. A FISA court order could capture communications for months between the target and his associates without his knowledge. All evidence is validly collected and can be used against the target in a domestic criminal case, simply because there is a foreign element involved, or a "significant purpose."

FISA's purpose is foreign intelligence gathering to protect national security and the ECPA includes the processes to gather evidence for domestic criminal prosecution. If FISA provides law enforcement an easy path to data collection, it will circumvent Congressional intent and that of President Carter who signed FISA into law in 1978. "It [FISA] will assure FBI field agents and others involved in intelligence-collection that their acts are authorized by statute and, if a U.S. person's communications are concerned, by a court order."[214] The war on terror should not provide a dragnet for law enforcement to incidentally catch criminals or invade the privacy of U.S. citizens in their electronic space.

---

[1] *See* Whitney Ray *Landline Decline,* Capitol News Service, August 2010. ("7.5 million Floridians still have landline telephones in their homes, but the number is falling fast. In Florida last year a million people canceled their landline service.").

[2] *See* Kevin Woodward *More Mobile Point-of-Sale Services Debut,* Payments Source, (October 2010), available at http://www.paymentssource.com/news/more-mobile-pos-services-debut-3003665-1.html.

[3] Electronic Communication Privacy Act of 1986 (ECPA), Pub. L. No. 99-508 100 Stat. 1848 (codified and amended as 18 U.S.C.A. §§ 2510-2522, 2701-2711 and 3121-3127) (WL October 2010).

[4] 18 U.S.C.A. §§ 2701-2711 (WL October 2010).

[5] *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 903 (2008).

[6] *See* Wikipedia, *Public Switched Telephone Network*, available at http://en.wikipedia.org/wiki/PSTN.

[7] *See* Margeurite Reardon, *Phone, Cable Companies Embracing Web 2.0,* CNET News, (November 2006), available at http://news.cnet.com/Phone,-cable-companies-embracing-Web-2.0/2100-1033_3-6133451.html.

[8] *See* Wikipedia, *Public Switched Telephone Network*, available at http://en.wikipedia.org/wiki/PSTN.

[9] *Id.*

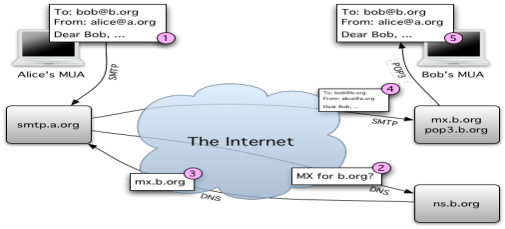
[10] Juniper Networks *Voice over IP 101*, p. 3 (May 2007).

[11] *See Id.* at p. 5. (a key component of telephone service is signaling. PSTN signaling systems include time division multiplexing (TDM) and private branch exchange (PBX), which enables devices to talk to each other. Similarly, VOIP networks require signaling as well and use different protocols such as session initiation protocol (SIP) to exchange IP message datagrams, to achieve the same results. A datagram is similar to an envelope or buffer, into which envelope or buffer information is placed and then shipped.).

[12] *See* Juniper Networks, *Voice over IP 101,* p. 6, (May 2007) (both PSTN and VOIP complete calls by connecting logical digital signal-0 (DS0) channels through the network, combined with pulse code modulation. PSTN will transmit the audio payload directly over a dedicated DS0 channel, VoIP networks transport the audio payload using shared network resources.)

[13] See Mary Meeker, *Internet Trends* Morgan Stanley Research (2009) available at http://www.ms.com/techresearch.

[14] *See* generally,Your Dictionary.com, available at http://computer.yourdictionary.com/store-and-forward ("A switch or router, for example, may have buffers to store incoming frames or packets of data until internal computational resources are available to process them and buffers to store outgoing frames or packets until bandwidth is available on a circuit in the forward direction. That way the device can mitigate issues of switch and circuit congestion. Messaging systems store voice, e-mail, and image (e.g., fax) messages when the intended recipient is unavailable and forwarding them on demand when the recipient is available."); *Modern Internet Email – How Email Works*, ISPTALK (2010), available at http://isptalk.co.nz/articles/electronic-mail.htm (see graphic below on email store and forward process).



[15] *See* generally Wikipedia, *How Email Works*, available at http://en.wikipedia.org/wiki/How_email_works#Operation_overview (typically, you write an email to someone's email address and hit "send" but what happens in the seconds before your email arrives at its destination? Your local mail user agent on your Mac or PC formats the message and uses simple mail transfer protocol (SMTP) to send the email message to a mail transfer agent (MTA), which will be at your ISP. The MTA looks at the destination address and looks up the domain name server address (DNS) unique IP address. The MTA resolves the address to a mailbox in the DNS and the DNS responds with a mail exchange (MX) record. The MTA sends the message to the MX using SMTP and it is delivered into the recipient mailbox, where she then requests it to come to her desktop machine/laptop using post office protocol POP3.).

[16] See Mary Meeker, *Internet Trends* Morgan Stanley Research (2009), available at www.ms.com/techresearch

[17] *See* Techcrunch, *A Comparison of Live Hotmail, Gmail and Yahoo Mail* (2007), available at http://www.businessinsider.com/chart-of-the-day-instant-messenger-services-2010-8.

[18] *See* ISP-Planet, *An ISP Guide to National and Global Providers*, available at http://www.isp-planet.com/resources/backbones/index.html.

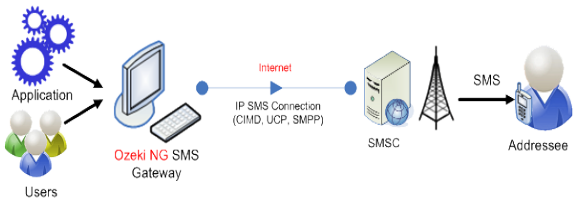
[19] *See* Pingdom, *Instant Messaging Facts and Figures* (2010), available at http://royal.pingdom.com/2010/04/23/amazing-facts-and-figures-about-instant-messaging-infographic/.

[20] *See* Wikipedia, *How Instant Messaging Works* (2010), available at http://en.wikipedia.org/wiki/How_email_works#Operation_overview.

[21] *See* Sybase Blog, *USA Now the Worlds Largest Generator of SMS*," (July 2009), available at http://blogs.sybase.com/wdudley/?p=537.

[22] *See* Wikipedia, *How Instant Messaging Works* (2010) (in order to text, you utilize a cell phone or peer to peer application and select a phone number of a recipient. When you type in a message under the SMS menu item and hit send, the message uses the nearest cell tower to send the message to a short message service center (SMSC) at the telco. From there, the SMSC contacts the home location register to find the recipient. Next, the message goes to a mobile switching center, which connects to a satellite for actual transmission of the message to the short message entity (SME). If the SME (pager, cell phone, etc.) is not active, the SMSC will store the message until it can be delivered to the recipient.).

[23] *IP SMS Connection,* SMS-Integration (2010) available at http://www.sms-integration.com/p_45-modem-vs-ip-sms.html (see diagram below of typical SMS communication).



[24] *See* ABA *Legal Technology Survey Results* (2010), available at http://www.abanow.org/2010/09/aba-legal-technology-survey-results-released/.

[25] *See* University of Colorado, *ASSETT Survey: Student Use of Communication Technology* (2009), available at http://assett.colorado.edu/post/160

[26] See Howrey LLP *President Signs Electronic Signature Act to Facilitate E-Commerce* (July 2000), available at http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/July_17_2000/e_signature.htm

[27] Warren & Brandeis, *The Right to Privacy*, 4 Harv.L.Rev. 193 (1890).

[28] *Id.*

[29] U.S. Const. amend. IV.

[30] *Silverman v. United States*, 365 U.S. 505, 511 (1961).

[31] *Id.*

[32] *Id.*

[33] *Katz v. United States*, 389 U.S. 347, 349 (1967).

[34] *Id.*

[35] *Id.* at 352.

[36] *Id.*

[37] *Id.*

[38] *Id.* at 351.

[39] *United States v. Miller*, 425 U.S. 435, 443 (1976).

[40] *Hoffa v. United States,* 385 U.S. 293, 302 (1966).

[41] *See United States v. James*, 353 F.3d 606, 614 (8th Cir. 2003). (computer discs were held in storage by a friend but that did not give control to the person such that they could consent to opening the package. The court cited the common carrier example.).

[42] *Wang v. United States,* 947 F.2d 1400, 1403 (9th Cir. 1991).

[43] *United States v. Poulsen* 41 F.3d 1330, 1335 (9th Cir. 1994).

[44] *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995).

[45] *United States v. Young*, 350 F.3d 1302, 1308 (11th Cir. 2003).

[46] *See* Health Insurance Portability and Accountability Act of 1996 (HIPPA), Pub. L. No. 104-191 § 1177(a), (HIPPA provides

protections for medial information provided to health insurance organizations.).

[47] *See United States v. Hambrick*, 55 F.Supp.2d 504, 508 (W.D.Va., 1999) (information given to an ISP is not private); U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, available at http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181 ("the U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment.").

[48] *United States v. Jacobsen*, 466 U.S. 109, 118 (1984).

[49] *United States v. Karo*, 468 U.S. 705, 708 (1984).

[50] *Id*.

[51] *Id.* at 717.

[52] *Kyllo v. United States*, 533 U.S. 27, 35 (2001).

[53] *Id.*

[54] *Id.* at 40.

[55] 18 U.S.C. § 2511(2)(a) (WL October 2010).

[56] *Id*. at § 2511(2)(a)(ii)(B).

[57] *Weeks v. United States*, 232 U.S. 383 (1914).

[58] *Herring v. United States* 129 S. Ct. 695, 701 (2009).

[59] *Id*. at 702.

[60] *Id*. at 708.

[61] *Smith v. Maryland*, 442 U.S. 735, 736 (1979).

[62] *Id.* at 745.

[63] *Id.* at 742.

[64] *United States v. Forrester*, 512 F.3d 500, 509 (9th Cir. 2008).

[65] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508. The Library of Congress, THOMAS. available at http://thomas.loc.gov/cgi-bin/bdquery/z?d099:HR04952:|TOM:/bss/d099query.html ("Summary of legislation - Title II: Stored Wire and Electronic Communications and Transactional Records Access - Makes it a criminal offense to: (1) willfully access, without authorization, a facility through which an electronic communication service is provided; or (2) willfully exceed an authorized access to such facility.

Prohibits the provider of an electronic communication service or remote computing service, except under certain circumstances, from divulging the contents of any communication stored, carried, or maintained by such service.

Sets forth the procedural requirements for a governmental entity to obtain access to electronic communications in electronic storage, including court-ordered back-up copies of the contents of such communications.

Allows any subscriber or customer of a communication service who is aggrieved by a willful or intentional violation of this Act to initiate a civil action to recover appropriate relief.

Grants the Director of the Federal Bureau of Investigation (FBI) access to telephone or communication service information and records relevant to any authorized foreign counterintelligence investigation. Prohibits any official or employee or a communications common carrier or service provider from disclosing to any person that the FBI has sought or obtained such access.

Establishes criminal penalties for interfering with the operation of a satellite.").

[66] *See Konop v. Hawaiin Airlines, Inc*., 302 F.3d 868, 875 (9th Cir. 2002). (the court discussed how the ECPA was drafted to protect privacy, when that website expected privacy through the use of a password.).

[67] *See Forrester*, 512 F.3d at 511.

[68] *Id.*

[69] 18 U.S.C. § 2703(a).

[70] *See* John McCallum, *Cost of Memory* (2008), available at http://www.jcmit.com/memoryprice.htm.

[71] 47 U.S.C. §§ 1001 et seq. (Lexis 2010).

[72] *See* Foreign Intelligence Surveillance Act of 1978 (FISA), Amendments Act of 2008. (codified in 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871) (Lexis 2008); *See* U.S. Department of Justice, Office of Justice Programs, Justice Information Sharing, available at http://www.it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop ("Like Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act"), the FISA legislation was the result of congressional investigations into Federal surveillance activities conducted in the name of national security. Through FISA, Congress sought to provide judicial and congressional oversight of foreign intelligence surveillance activities while maintaining the secrecy necessary to effectively monitor national security threats. FISA was initially enacted in 1978 and sets out procedures for physical and electronic surveillance and collection of foreign intelligence information. Initially, FISA addressed only electronic surveillance but has been significantly amended to address the use of pen registers and trap and trace devices, physical searches, and business records.").

[73] 18 U.S.C. § 2701.

[74] Pub. L. No. 99-508 (October 1986).

[75] 18 U.S.C. § 2510(15).

[76] *See* Internet Law Treatise *Privacy: Wiretap Act*, Electronic Frontier Foundation, (citing H.R. Rep. No. 99-647, at 35 (1986), available at http://ilt.eff.org/index.php/Privacy:_Wiretap_Act.

[77] *See* 18 U.S.C. § 2711(2) (further, the electronic computer system is defined in §2510(14) as " any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.").

[78] *See FTC v. Netscape Communications Corp*., 196 F.R.D. 559, 560 (N.D. Cal. 2000); *Freedman v. America Online, Inc*., 325 F. Supp. 2d 638, 643 n.4 (E.D. Va. 2004); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-15 (3d Cir. 2004).

[79] *See Fraser*, 352 F.3d at 112.

[80] *See Bohach v. City of Reno,* 932 F. Supp. 1232, 1235 (D. Nev. 1996).

[81] *See Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996). (email accessed from another company's bulletin board service did not make Sega an ECS with respect to that communication).

[82] *Crowley v. Cybersource Corp*., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001).

[83] 18 U.S.C. § 2702(a).

[84] *See Google Docs get File Storage: Is this the G Drive?*, CNET (January 2010) available at http://news.cnet.com/8301-27076_3-10432746-248.html.

[85] *See* 18 U.S.C. § 2511. (the statute focuses on the different ways that a communication may be intercepted, so anything in transit could potentially be intercepted and the prohibitions are set forth here).

[86] *See Id.* at § 2510(17).

[87] *See Id.* at § 2510(8).

[88] *See Id.* at § 3121.

[89] *See Id.* at § 2703(c)(2)(A-F).

[90] *See Id.* at. § 2703(c)(1).

[91] *See Id.* at § 2703(b)(1)(b) and § 2705 (the delayed notice provision).

[92] *See Id.* at § 2703(a) and (b).

[93] *See Id.* at § 2703(b).

[94] *See Id.* at § 2705(a).

[95] *See Id.* at § 2703(a).

[96] *See Crispin v. Christian Audigier, Inc*., 2010 U.S. Dist. LEXIS 52832, at 7.

[97] *See Phone Records Surveillance is Widely Acceptable to Public*, ABC News (May 2006) available at http://abcnews.go.com/Politics/story?id=1953464.

[98] *See Theofel v. Farey-Jones*, 341 F.3rd 978, 981 (9th Cir. 2003).

[99] *Id*. at 982.

[100] *See Id*. (the court referenced the Computer Security and Abuse Act).

[101] *See Id*. at 984.

[102] *See Theofel*, 341 F.3rd at 985.

[103] *In Re Doublick, Inc. Privacy Litig*., 154 F. Supp. 2d 497 (S.D.N.Y., 2001); *Fraser v. Nationwide Mut. Ins. Co*., 135 F.Supp.2d 623 (E.D.Pa., 2001); *Steve Jackson Games, Inc. v. U.S. Secret Serv*ice, 36 F.3d 457 (5th Cir., 1994).

[104] *See United States v. Weaver* 636 F.Supp.2d 769 (C.D.Ill., 2009).

[105] *Id*. at 773.

[106] *See Weaver*, 636 F. Supp.2d at 773.

[107] *See Steve Jackson Games, Inc*., 36 F.3d at 461; *United States v. Councilman*, 245 F. Supp. 2d 319 (D. Mass. 2003), aff'd, 373 F.3d 197 (1st Cir. 2004), rev'd, 418 F.3d 67 (1st Cir. 2005).

[108] *See Fraser*, 352 F.3d at 114.

[109] *See Bansal v. Russ*, 513 F.Supp.2d 264, 274-277 (E.D.Pa., 2007).

[110] 18 U.S.C. § 2711 (October 2009).

[111] *United States v. Szymuszkiewicz*, 2009 WL 1873657, at *10, (E.D.Wis.,2009) ("Given the broad definition of stored communications, these courts further concluded that even that temporary storage incidental to the transmission process took an e-mail outside the coverage of the Wiretap Act….The statutory language does not support the inferential leap taken by these courts. As indicated above, the definition of "electronic communication" contains specific exclusions, but "electronic storage" is not one of them").

[112] *Bailey v. Bailey*, No. 07-11672, 2008 US Dist. Lexis 8565 (E.D.Mi., 2008).

[113] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, The Library of Congress, THOMAS, available at http://thomas.loc.gov/cgi-bin/bdquery/z?d099:HR04952:|TOM:/bss/d099query.html ("Title I: Interception of Communications and Related Matters - Amends the Federal criminal code to extend the prohibition against the unauthorized interception of communications to include specific types of electronic communications.").

[114] 18 U.S.C. § 2510(4) ("intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device).

[115] 18 U.S.C. § 2510(1) ("wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.).

[116] 18 U.S.C. § 2510(2) ("oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.).

[117] *See Privacy: Wiretap Act*, Internet Law Treatise, Electronic Frontier Foundation available at http://ilt.eff.org/index.php/Privacy:_Wiretap_Act. (citing 18 U.S.C. § 2518(3)(a)-(b)).

[118] 18 U.S.C. § 2515.

[119] *United States v. Kennedy*, 81 F.Supp.2d 1103, 1111 (D.Kan., 2000).

[120] *United States v. Scarfo*, 180 F.Supp.2d 572, 578 (D.N.J., 2001) (noting that 18 U.S.C. § 2510 would not apply).

[121] *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir., 2005).

[122] *Id.*

[123] See Top Ten Reviews, *Monitoring Software Review*, (2010) available at http://monitoring-software-review.toptenreviews.com/.

[124] *Hall v. Earthlink Network, Inc*., 396 F.3d 500, 505 (2nd Cir., 2005).

[125] *Id.*

[126] *See* Out-law.com, *ISP and Web Host Conditions: Checklist*, (2008) available at http://www.out-law.com/page-5710.

[127] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508. The Library of Congress, THOMAS, available at http://thomas.loc.gov/cgi-bin/bdquery/z?d099:HR04952:|TOM:/bss/d099query.html (summary "Title III: Pen Registers and Trap and Trace Devices - Prohibits the installation or use of a pen register or a trap and trace device without a court order pursuant to this Act or under the Foreign Intelligence Surveillance Act of 1978. Imposes criminal penalties for violations of such prohibition.

Authorizes Government attorneys and State law enforcement officers to apply for a court order allowing the installation and use of a pen register or a trap and trace device. Allows the issuance of such an order if the attorney or law enforcement officer certifies that information likely to be obtained by such installation is relevant to an ongoing criminal investigation.

Requires providers of wire communications, landlords, custodians, and other persons to furnish all information, facilities, and technical assistance necessary to accomplish the installation of a pen register or a trap and trace device if such assistance is ordered by the court. Requires that anyone providing such assistance be compensated for any reasonable expenses incurred. States that no cause of action shall lie in any court against anyone providing such assistance.

Requires the Attorney General to report annually to the Congress on the number of pen register and trap and trace device orders applied for by law enforcement agencies of the Department of Justice.").

[128] 18 U.S.C.A. § 3127(4) (WL October 2009).

[129] *Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir., 1995).

[130] *See* Center for Democracy & Technology, available at http://www.cdt.org/, (the URL reveals the whole document. Such revealing information appears in other addresses: If you search Yahoo for information about "FBI investigations of computer hacking," the addressing information you send to Yahoo includes your search terms. The URL looks like this: http://search.yahoo.com/bin/search?p=FBI+and+hacking+investigations.").

[131] *See The Wiretap Report,* U.S. Courts (2009) available at http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2009.aspx.

[132] *Gonzalez v. Google* 234 F.R.D. 674 (N.D.Cal., 2006).

[133] *Id*. at 688.

[134] Charlie Savage, *Wiretapped phones, now Internet?*, New York Times, (September 2010) available at http://www.startribune.com/nation/103836983.html.

[135] *Leventhal v. Knapek*, 266 F.3d 64, 73 (2nd Cir., 2001).

[136] *O'Connor v. Ortega* 480 U.S. 709, 720 (1987).

[137] *Id.*

[138] *Id.* at 729.

[139] *U.S. v. Ziegler*, 474 F.3d 1184, 1189 (9th Cir., 2007).

[140] *Warshak v. United States*, 532 F.3d 521, 525 (6th Cir., 2008). (the court allowed the use of §2703(b)(1)(B) for 90 day delayed notices in succession).

[141] *Id.* at 531.

[142] *Forrester*, 512 F.3d at 509 (*Forrester* informs that the email content should be protected like letters but the To/From addressing on emails is like the Pen Register information).

[143] *Id.*

[144] *Pure Power Boot Camp v. Warrior Fitness Boot Camp, LLC*, 587 F.Supp.2d 548, 555 (S.D.N.Y., 2008).

[145] *Id.*

[146] *Id.* at 561.

[147] *Quon v. Arch Wireless Operating Co., Inc*., 529 F.3d 892, 903 (9th Cir., 2008).

[148] *Id.* at 901.

[149] *Id.* at 903.

[150] *O'Connor* 480 U.S. at 725.

[151] *Quon*, 529 F.3d at 904.

[152] *Id.* at 897. (text messages would not be investigated as long as the employee paid for any overages).

[153] *Id.* at 909.

[154] *City of Ontario v. Quon,* 130 S.Ct. 2619 (2010).

[155] *Id*. at 2623.

[156] *See Id*. at 2630 ("A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds. For present purposes we assume several propositions *arguendo:* First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City; second, petitioners' review of the transcript constituted a search within the meaning of the Fourth Amendment; and third, the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere.").

[157] *Id*. at 2621.

[158] *See Is P2P Dying or Just Hiding?* CAIDA (2004) available at: http://www.caida.org/publications/papers/2004/p2p-dying/p2p-dying.pdf.

[159] *Id.*

[160] 47 U.S.C. § 1001 (1998) available at http://www.fcc.gov/calea/ ("CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities. Common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service – all three types of entities are defined to be "telecommunications carriers" for purposes of CALEA section 102, 47 U.S.C. § 1001 – must comply with the CALEA obligations set forth in CALEA section 103, 47 U.S.C. § 1002.").

[161] 18 U.S.C.A. § 2522(a) (WL 1996).

[162] *See Second Report and Order and Memorandum Opinion and Order (Order*), FCC (2006) available at http://www.fcc.gov/Forms/Form445/445.pdf ("Seventh, the Order concludes that carriers are responsible for CALEA development and implementation costs for post-January 1, 1995 equipment and facilities, and declines to adopt a national surcharge to recover CALEA costs. The Order finds that it would not serve the public interest to implement a national surcharge because such a mechanism would increase the administrative burden placed upon the carriers and provide little incentive for them to minimize their costs.").

[163] Charlie Savage, *U.S. Pushes to Ease Obstacles to Wiretapping* N. Y.Times (October 2010) available at http://www.topics.nytimes.com.

[164] *See Id.* ("The push to expand the 1994 law is the latest example of a dilemma over how to balance Internet freedom with security needs in an era of rapidly evolving — and globalized — technology. The issue has added importance because the surveillance technologies developed by the United States to hunt for terrorists and drug traffickers can be also used by repressive regimes to hunt for political dissidents…. Starting in late 2008 and lasting into 2009, another law enforcement official said, a "major" communications carrier was unable to carry out more than 100 court wiretap orders. The initial interruptions lasted eight months, the official said, and a second lapse lasted nine days. This year, another major carrier experienced interruptions ranging from nine days to six weeks and was unable to comply with 14 wiretap orders. Its interception system "works sporadically and typically fails when the carrier makes any upgrade to its network," the

official said.").

[165] Jeri Clausing, *FCC Suggests V-Chips for PCs* N.Y. Times (1997) available at http://www.nytimes.com/library/cyber/week/103097vchip.html ("The FCC, however, insists that the proposal has nothing to do with the Internet. In fact, one agency official said, the V-chip would not even work on Internet content or video streaming technology.").

[166] USA PATRIOT ACT OF 2001 Pub. L. No. 107-56, 107th Congress (2001).

[167] 50 U.S.C.A. § 1801 Foreign Intelligence Surveillance Act of 1978 (WL July 2008).

[168] 50 U.S.C.A. §1801(b) (WL July 2008); §1801(b)(2) (the test for an American to be an agent of a foreign power, is "if he knowingly engages in or conspires in illegal clandestine intelligence gathering, sabotage, or terrorism, or assumes a false identity for or on behalf of a foreign power); §1804 (unlike the warrant process, to get a surveillance order, an application is made to the Foreign Intelligence Surveillance Court (FISC) and the applicant must claim that this information cannot be gathered using the normal investigative techniques and is foreign intelligence); §1805(a)(5) (The Attorney General must approve the application and the "probable cause standard is that the certifications in the application are not clearly erroneous)..

[169] I*d.* at §1801(f); FRCP 41(b)(3), (5) (the warrant test looks to criminal activity, "[i]n an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district. (5) "[a] magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property.").

[170] 50 U.S.C.A. § 1801(b)(2)(A) (WL July 2008) (this statute only requires that the target is "knowingly engage[d] in clandestine intelligence gathering activities.").

[171] *Id*. at §1806(c) (the government only provides notice if it plans to use the evidence collected in trial. "[t]he Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.").

[172] *Id.* at § 1805(c).

[173] *Id.* at § 1805(a)(3)(B).

[174] 18 U.S.C. §§ 2332(f),(g),(h).

[175] 50 U.S.C.A. § 1801(c)(2).

[176] 50 U.S.C.A. § 1802 (a)(1).

[177] 18 U.S.C. §§ 2510(14), 2703.

[178] 18 U.S.C. § 2703(c)(2).

[179] 18 U.S.C. § 3103a(b).

[180] 50 U.S.C. §1842(a)(1).

[181] 50 U.S.C. §1804(a)(6)(B).

[182] *Id*.

[183] *In Re Sealed Case*, No. 02-001, 310 F.3d 717 (For.Intel.Surv.Rev., 2002).

[184] *Id.* at 746.

[185] *Id*.

[186] U.S. Dept. of Justice, Office of Legislative Affairs (April 2010) available at http://www.justice.gov/nsd/foia/reading_room/2009fisa-ltr.pdf ("This report is submitted pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the "Act"), as amended, 50 U.S.C. § 1801 *et seq.,* and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006). In accordance with those provisions, this report covers all applications made by the Government during calendar year 2009 for authority to conduct electronic surveillance for foreign intelligence purposes under the Act.").

[187] 18 U.S.C. § 2709(a) (WL March 2006).

[188] 50 U.S.C. § 1801(h)(3).

[189] *See Katz*, 389 U.S. at 360 (in concurring opinion, Justice Douglas discusses the importance of keeping the Executive Branch separate from the Judiciary, when gaining access to communications of criminals of any sort. "The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases. They may even be the intended victims of subversive action. Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.").

[190] *Mayfield v. United States*, 504 F.Supp.2d 1023 (D.Or., 2007)

[191] *Id.* at 1028.

[192] *Mayfield,* 504 F.Supp.2d at 1032.

[193] *Id.*

[194] *Mayfield* 599 F.3d at 973.

[195] *United States v. Warsame*, 547 F.Supp.2d 982, 996 (D.Minn., 2008); Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511, S-1566 (1978) (original authority for scope of wiretaps under FISA was narrowly directed at foreign agents and activity and was careful to exclude Americans. *See* Sec. 102. codified as 50 USC § 1802 (a)(1) "Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that--,

(A) the electronic surveillance is solely directed at--,

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a) (1), (2), or (3); or (ii) the acquisition of technical intelligence other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a) (1), (2), or (3);

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party;

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to--,

(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 103, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power **for the purpose of obtaining foreign intelligence information,** except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1) (A) of subsection (a) unless such surveillance may involve the acquisition of communications of any United States person.").

[196] Senator Hatch (UT), *The U.S.A. Patriot Act in Practice: Shedding Light on the FISA Process,* Congressional Record (September 24, 2002) p. S9109-S9110 available at http://www.fas.org/irp/congress/2002_cr/hatch-fisa.html (in discussing the post September 11th changes to FISA in the U.S. Senate. "Prior to the U.S.A. PATRIOT Act of 2001, the Foreign Intelligence Surveillance Act of 1978 authorized the government to gather intelligence on agents of foreign powers with less stringent requirements than those required for surveillance of domestic criminals. The courts interpreted FISA as requiring that gathering foreign intelligence be the "primary purpose" of the surveillance of the foreign agent. *See United States v. Duggan*, 743 F.2d 59, 77 (2nd Cir. 1984); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), cert. denied, 454 U.S. 1154 (1982).

This statutory regime worked well during the cold war for conducting surveillance on spies who were either foreign nationals employed by foreign government working under diplomatic cover at foreign embassies in the United States, or United States persons in this country who had been recruited to spy by foreign intelligence agencies. Both were clearly "agents of a foreign power," and gathering foreign intelligence on the activities of these targets was generally the "primary purpose," if not the only purpose, of the surveillance. The statutory regime did not work as well with respect to terrorists, who did not work for a foreign government, who often financed their operations with criminal activities, such as drug dealing, and who began to target American interests. It was more difficult to determine if such terrorists were "agents of a foreign power" and it was difficult for the government to keep the appropriate types of investigators, intelligence or criminal, involved in the operation.

To determine what the "primary purpose" of a surveillance was, courts looked to what type of federal investigators were managing and directing the surveillance operation. If intelligence investigators managed and directed the surveillance, courts interpreted the primary purpose of the surveillance to be gathering foreign intelligence, thus requiring the government to comply with the less stringent FISA surveillance procedures. On the other hand, if criminal investigators managed and directed the surveillance, courts interpreted the primary purpose of the surveillance to be gathering criminal evidence, thus requiring the government to comply with the more stringent Title III wiretap procedures or to exclude the evidence from court.

In short, the courts held that there could be only one primary purpose, and it was either gathering foreign intelligence or gathering criminal evidence. *See*, e.g., *Truong*, 629 F.2d at 912-13."); Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008). (amended language Sec. 702 (g)(2)(v) "Requirements. A certification made under this subsection shall

"(A) attest that—

"(v) a significant purpose of the acquisition is to obtain foreign intelligence information.").

[197] *Smith* 442 U.S. at 749 (MARSHALL, J., dissenting).

[198] *See Master Services Agreement*, Exodus Communications Inc. and Geocities (Nov 07, 1997) available at http://contracts.corporate.findlaw.com/operations/services/327.html.

("Exodus represents that it exercises no control over the content of the information passing through its Internet Data Centers").

[199] *In Re U.S.* 665 F.Supp.2d 1210, 1217 (D.Or., 2009) (defining notice for access to data held by an RCS, 18 U.S.C. § 2703(b)(1)(A) "without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." In discussing FRCP § 41(f)(1)(C) need for notice to actual subscriber or just the ECS, "[t]he 2002 Amendments provide: Amended Rule 41(e)(2)(B) is a new provision intended to address the contents of tracking device warrants. To avoid open-ended monitoring of tracking devices, the revised rule requires the magistrate judge to specify in the warrant the length of time for using the device. Although the initial time stated in the warrant may not exceed 45 days, extensions of time may be granted for good cause. The rule further specifies that any installation of a tracking device authorized by the warrant must be made within ten calendar days and, unless otherwise provided, that any installation occur during daylight hours.

Under the FRCP Rule 41, Warrant for a Tracking Device, there is a requirement for notice to the person who has been tracked or their property has been tracked. FRCP 41(f)(2)(c) Service. Within 10 calendar days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was

tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in Rule 41(f)(3).").

(3) Delayed Notice. Upon the government's request, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--may delay any notice required by this rule if the delay is authorized by statute.").

[200] *Id.* at 1222.

[201] *Id.* (because the email is in multiple locations at once, there has been no meaningful interference with the property and no notice is triggered under FRCP 41).

[202] *Id.* at 1224.

[203] *California v. Greenwood*, 486 U.S. 35, 41 (1988).

[204] *United States v. Freitas* 800 F.2d 1451, 1455 (9th Cir., 1986) (discussing that Rule 41(h) is not limited to tangible items).

[205] 18 U.S.C. § 2518 (8)(d) (WL Oct. 1998).

[206] *In Re U.S. for an Order Authorizing Installation and Use of a Pen Register*, 415 F.Supp.2d 211, 214 (W.D.N.Y., 2006).

[207] 18 U.S.C. § 3122(b)(2) (WL 1996).

[208] 47 U.S.C. § 1002(a)(2) (WL1998) ("[e]xpeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier…..except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number.").

[209] 18 U.S.C. § 2703(d) (WL 2009).

[210] *In Re,* at 215.

[211] *See In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace,* 2005 WL 3471754 (S.D.N.Y., 2005); *In the Matter of the Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device and Authorizing Release of Subscriber Information and/or Cell Site Information,* 2006 WL 244270 (W.D.La., 2006.).

[212] Simmons, Joshua L., *Buying You: The Government's Use of Fourth-Parties to Launder Data about 'The People'* (September 2009) Colum. Bus. L. Rev., Vol. 2009, No. 3, p. 950.

[213] Jeff Jonas *Your Movements Speak for Themselves: Space-Time Travel Data is Analytic Superfood!* (August 2009) available at http://jeffjonas.typepad.com/jeff_jonas/2009/08/your-movements-speak-for-themselves-spacetime-travel-data-is-analytic-superfood.html

[214] John Woolley and Gerhard Peters, *Foreign Intelligence Surveillance Act of 1978 Statement on Signing S. 1566 Into Law,* The American Presidency Project (October 1978) available at http://www.presidency.ucsb.edu/ws/index.php?pid=30048 ("This is a difficult balance to strike, but the act I am signing today strikes it. It sacrifices neither our security nor our civil liberties. And it assures that those who serve this country in intelligence positions will have the affirmation of Congress that their activities are lawful.").