

Know Your Enemy: Know Your Lawyer

by David Dittrich and Alisha Ritter

DRAFT (DO NOT REDISTRIBUTE AT THIS TIME)

I am not an advocate for frequent changes in laws and institutions. But laws and institutions must go hand-in-hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with change of circumstances, institutions must advance also to keep pace with the times.

Letter from Thomas Jefferson to Samuel Kercheval, 1816

Introduction

This paper is intended to be a legal overview for private, educational, and corporate entities setting up and using Honeynets. Honeynets are networks of honeypots, and are described in detail in the paper, Know Your Enemy: Honeynets (found at <http://project.honeynet.org/papers/honeynet/>). It is assumed that the reader is familiar with the contents of this paper.

The information in this paper is not to be relied upon by law enforcement or its agents, or by the military, telecommunication industry, etc. (In short, this is not for any entity specifically named or described in communications privacy legislation.) If you are going to share information about your Honeynet with law enforcement, carefully review what you intend to share with your legal advisors. There are complicated restrictions on what kinds of communications may be shared legally; evidence cannot be presented in court if it is obtained illegally.

The goals of this paper are to illustrate the various United States criminal and civil statutes as they relate to computer intrusions, monitoring, and other activities performed by system administrators, network operators, security incident response teams, and security researchers using Honeynet or honeypot style technologies. It is also intended to show relationships between various privacy laws at the federal level, relationships between federal and state statutes, and places where federal and state laws cause “gray areas” between actions of malicious attackers and responsible defenders.

This paper starts out with by explaining the federal laws that apply to electronic communications privacy and computer intrusion in the United States. It then goes on to show a typical attack/defend scenario, and how these laws apply to the actions of the attacker and defender. Afterwards, the difference between a typical attack/defend scenario and that of a research honeynet is shown to illustrate some of the “gray areas” in current law. We end with some analysis of existing proposals for changes in the privacy statutes that have been made by legal minds around the US.

Laws

Types Of Data

Federal and state laws look at four primary types of data associated with private electronic communications:

Transactional records about communication,

1. Acquired in real-time, or
2. Accessed in stored (or historical) form

Content of communications,

3. Acquired in real-time, or
4. Accessed in stored (or historical) form

Transactional records are things like IP addresses, ports, network protocols, account names, email header information (except the Subject: line), time/date, URLs, etc.

Content of communications is the full email header (including Subject: line), the body of email messages, file contents, full packets captured on a network segment, reconstructed content of interactive sessions (e.g., IRC chat, commands executed in a shell account, typed passwords), etc.

There is a legal distinction between communication that is captured in transit over a communication medium (such as listening in on wireless telephone frequencies or examining TCP packets sent over an Ethernet network) and data that is stored in a file system for longer periods of time (such as email folders, system logs, and executable program files.)

Primary Federal statute about Computer Fraud and Abuse

The Computer Fraud and Abuse Act (18 USCS § 1030) is considered the primary federal anti-hacking statute. It is the computer administrator's first defense against unauthorized access, or authorized access that was exceeded.

Primary Federal statutes about privacy of Electronic Communications

The 4th Amendment to the United States Constitution is often brought up in the context of privacy, but this is usually not applicable to honeypots. The reason for this is that the Bill of Rights is designed to protect U.S. citizens against abuses by the government. In that context, it is a defense against criminal prosecution and is used to exclude evidence in a criminal trial. It has no civil penalties (you can't sue an individual in civil court for violating your 4th Amendment rights.) That said, only agents of law enforcement need be concerned about 4th Amendment abuse, so these protections do not apply to most honeypots.

What the rest of us must be aware of are state and federal laws that protect the privacy of communications from unauthorized monitoring by other citizens (including, but not limited to, law enforcement).

There are three main statutes at the Federal level that govern unauthorized monitoring. These are:

1. Wire and Electronic Communications Interception and Interception of Oral Communications (Title III, 18 USC § 2510-22), commonly known as "Wiretap."
2. Stored Wire and Electronic Communications and Transactional Records Access (18 USC § 2701-11), commonly known as "ECPA."
3. Pen Registers and Trap and Trace Devices (18 USC § 3121-27), commonly known as "Pen/Trap."

These statutes are very complicated. All three attempt to define when monitoring is illegal, and provide exceptions for when it might be legal. The rules depend on the type of electronic data being gathered and the methods used (i.e. transactional or content, and real-time or stored). A more thorough treatment of these laws is included at the end of this paper.

It should also be noted that the USA Patriot Act, passed in October 2001 as House Resolution 3162, changed some of the language of these three statutes, but in the context of law enforcement. The changes were intended to clarify and expand older legislation that was written when radios, telephones and telegraphs were the only means of communication. The Patriot Act includes language that applies to the Internet, email, real-time messaging, chat, international communication, and computer crime. It addresses situations where someone acting under "color of law" (i.e., law enforcement) can monitor private communications in pursuit of a criminal, and it also simplifies obtaining and executing of search warrants for transactional records when tracking a criminal who is using telecommunications or computing systems in multiple jurisdictions.

[Example provided by Richard Salgado: Let's say there is an intruder on the system who creates his or her own account, or steals someone else's, and begins to use it to, say, send e-mail. If the system administrator catches this and creates a clone account so that every time an e-mail goes in or out from the hacked account, a copy is made and put in the cloned account. The system administrator is intercepting the contents of the attacker's communications in real time. If the system administrator looks at the e-mails, not from the cloned account, but in the intruder's "sent mail," then the sys admin has acquired the contents of communications that were stored. If instead of creating a cloned account, the monitoring kicked on and only logged only the incoming IP then the sys admin would be intercepting transactional data in real time. Depending on the type of data collected and the method of collection, different rules apply.]

To give you a preview: Real Time interception of the contents of communications means the Wiretap Act applies. Real time interception of transactional information means the Pen Register/Trap and Trace statute applies. Access to the contents of communications OR transactional information means that ECPA applies – except that many portions of ECPA govern only entities that provide electronic communications services to the public, like AOL, and probably will not apply to honeypots. This is a hard area of the law, but we can do it.]

A Typical Attack/Defend Scenario

You are the administrator of a computer system, or a member of the security incident response team for your organization. Or perhaps you are a computer security researcher who analyzes computer security tools and tactics and publishes the results for the benefit of the Internet community. Either way, one of your main goals is the protection of the computers under your authority from abuse by unauthorized intruders.

In setting up your computer systems, you installed login banners¹ on your systems, which say something like,

“This system is for the use of authorized users only. By using this computer, you are consenting to have all of your activities on this system monitored and disclosed to others, including law enforcement. Keep out.”

[Consent? What if they don't hit a service with a banner?]

Meanwhile, somewhere in the world a computer criminal launches a program designed to automatically locate, penetrate, and conceal evidence of an intrusion through replacement of operating system commands (using a “root kit”). When the attack is over, she may “own” hundreds, perhaps even thousands of computers around the world.

Not only does the criminal want control of the systems, she might also install a “sniffer” program (or a Trojan horse version of the SSH daemon) to gather passwords for more accounts on other systems, extending her reach into your and other networks. She also wants to run a TCP port redirector (generically known as “BNC” or bounce) to hide her true location on the Internet. Or she might want to run an Internet Relay Chat (IRC) “bot” program to give her 24x7 control of the private IRC channels she and her team can use to discuss intrusions, trade credit cards and stolen accounts, obtain new exploits, and develop their tools.

At some point, she or her team members’ activity becomes a little too noisy, and someone notices. You may have seen an alert from your Intrusion Detection System (IDS) that scanning was detected, or that an exploit’s shell code was found in your network traffic. Someone at another site may have discovered a password no longer works and reported that logins to the suspect account originate from an IP address at your site. You may get a report of a denial of service attack flood, part of which is originating from IP addresses on your network. Whatever it is that tips you off, you still don’t know which systems may have been (were) compromised, who did it, what they did, and what you have to do to fully remove their unauthorized access and presence from your network.

You now go looking for evidence that confirms your suspicions. You review your network traffic logs from your IDS, your firewall. Once you have one or more suspect IP addresses, you may scan them externally to see what services are running on them. Then you compare that with what the system owner reports is visible from within the system. At this point, you are only gathering data that shows IP addresses (sources and destinations), ports, times, etc. This is referred to as “transactional data,” and its interception in real-time is covered by the Pen/Trap Statute.

You now know which host or hosts are likely compromised and out of your control. Now you may choose to start using tcpdump to capture a full packet dump of *all* traffic to/from the suspect host(s). You are now doing real-time interception of electronic communications, which is covered by the Wiretap Statute.

After analyzing the network traffic and identifying which systems are compromised, you know they are running IRC bouncers or bots, you know they have backdoor encrypted shells running on non-privileged (and non-standard) ports. You may remove the systems from the network at this time and get a bit-image copy of the hard drive. You also start to analyze a copy of the file system to locate all the intruder’s modifications to your operating system, as well as any programs, IRC logs, email, etc. placed on your system by the intruder. You are now obtaining copies of stored communication on your systems, which is covered by the ECPA.

This above scenario plays out daily, at thousands of sites around the world. In many cases, these systems are live, production systems that provide real services, to real users, who are doing real work, communicating with friends and family, or being entertained. In other cases, the systems may be privately owned and operated only for the purpose of researching the methods and tactics of computer intruders.

Depending on who owns the computers and what they are used for, various laws – and their subsections - apply differently. These laws exist at both the state and federal level, and sometimes may conflict or be more/less restrictive. Things can get very complicated and ambiguous, depending on who you are, how/what you are doing, and why.

Now let’s look at various aspects of the scenario above, point by point, and try to understand the legal dimensions.

Action Matrix

Action	Actor	Related statute
--------	-------	-----------------

Which laws apply

Protection of computer systems

The first law that applies to this scenario is the Computer Fraud and Abuse Act (CFAA). It provides penalties for intentionally accessing (or attempting to access) protected computers. Collecting the evidence needed to prove this is where the privacy laws (Wiretap, ECPA, and Pen/Trap) become indispensable.

Each of the privacy statutes listed above has an exception for providers of electronic communication services (ECS) and remote computing services (RCS), when they are acting to protect their systems by monitoring electronic communications. Whether a site falls under the definition of an ECS and/or RCS provider is important,² and systems that do not provide any services what so ever to the public may not be considered either.³ State laws may be even more restrictive about who qualifies as a “service provider.” So even in the case of protecting a computer system owned by a private citizen or government agency, you may be violating privacy laws by monitoring network traffic.

Importantly, anyone who provides the means of communicating electronically can be a provider of electronic communications, even if they are doing so for themselves.⁴ The main point is that the hacked entity must provide the ability to send or receive the precise communication at issue. You cannot provide ECS with respect to a communication if you do not provide the ability to send or receive that communication.^{5 6}

Banners and implied consent

Another important exception to the restrictions on intercepting electronic communications is where one of the parties to communication consents to monitoring of that communication. The federal statutes employ “one party consent,” which means that only one party to the communication must consent for monitoring to legally take place. State law may be more restrictive; however, in Federal courts, Federal laws apply.

In a hacking scenario, there are inherent difficulties in determining who is technically a party to the communication. There are a few cases that generally support the idea that the owner of a computer system may satisfy the “party to the communication” consent language when a user sends communication to the owner’s system.⁷ Banners, such as the one described above, may indicate that the owner of the system retains the right to monitor all communication on their system, and anyone who continues to use that system after seeing that banner implies consent to this monitoring.

Banners help establish the user’s consent to real-time monitoring under Section 2511(2)(d), and the retrieval and disclosure of information stored on the network under Sections 2702(b)(3) and 2703(c)(1)(B)(iii). Making users click through banners helps indicate that the consenting party has received notice of the monitoring. However, there may be a question of whether someone who cannot read the banner (e.g., a non-English speaker) or who breaks in through a non-interactive service, and does not produce a banner on use (e.g. Remote Procedure Call, or RPC), has implied consent.

Consent to monitoring cannot be coerced or induced. It must be voluntary.

Computer Trespass and Malicious intent

In a state case, *State of Washington v. Riley*, Joseph Riley was convicted of Computer Trespass for using his home computer to dial into the telephone switch of a telephone operator in Washington and repeatedly trying pass codes to allow him to make fraudulent telephone calls.⁸ The attempts were discovered by the telecommunications company, who reported the activity to their telephone provider. The telephone provider installed a line trap to allow them to trace the calls, which lead to Riley’s home telephone number. Riley’s home was searched, and a script for trying pass codes, notes of Riley’s activity, and four access codes were found. Riley confessed to attempting to gain unauthorized access to the switch’s pass codes.

Washington Law (RCW 9A.52.110) states:

“[a] person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another...”

The term “access” is defined as, “to approach ... or otherwise make use of any resources of a computer, directly or by electronic means.” Repeatedly dialing in and trying pass codes was deemed by the court not to be simply calling the switch, but “accessing” the switch. Riley was therefore trespassing on the computer.

In an analogous way, someone who is doing broad, automated scans of wide network address ranges, and attempting to exploit remote vulnerabilities on those systems to gain access, is engaging in the same kind of behavior indicative of malicious intent to trespass on computer systems.

Coincidentally for this discussion, Riley appealed his conviction on grounds that the trap device recorded a “private communication” (the number being called and time), in violation of Washington’s privacy law, RCW 9.73.030(1)(a), which states:

“[I]t shall be unlawful for any ... corporation ... to intercept, or records any: (a) Private communication transmitted by telephone ... between two or more individuals... by any device electronic or otherwise designed to record and/or transmit said communication regardless of how such device is powered or actuated, without first obtaining the consent of all the participants in the communication[.]”

He argued that another case, *State v. Gunwall*, 106 Wn.2d 54, 720. In *Gunwall*, the court held that a pen register

Real-time interception of transactional records

The Pen/Trap statute deals with real-time transactional communications. In our scenario above, there are two points at which real-time interception of transactional records occurred.

The first is when our attacker installed a Trojan horse SSH daemon on the system. Since SSH encrypts traffic during a login session, a normal sniffer will be unable to capture the password of a user as a remote login occurs. A common tactic right now is to gather account names and passwords to replace the existing SSH daemon with one that has modifications to log the time, source computer, account name, and password used for a login. The log (as shown in the Forensic Challenge⁹ intrusion) looks like this:

```
+-[ User Login ]----- - - - - -
| username: root password: tw1Lightz0ne hostname: c871553-b.jffsn1.mo.home.com
+----- - - - - -
```

Our intruder in no way has authority or permission to intercept these transactional records, and is thus in violation of the Pen/Trap statute.

The second point at which real-time interception of transactional records occurs is when the IDS and firewall logged the incoming connections from the attacker’s last stepping stone. The IDS and firewall, however, are an integral part of the security system used to protect the systems in the Honeynet. The banners on the system re-enforce in the minds of anyone using the system that monitoring may occur for protective purposes. They are thus legal to use for this purpose.

Real-time interception of content of communications

The Wiretap Act covers real-time interception of the content of communications. Again, there are two points in our scenario when real-time interception of the content of communications occurred.

First, the attacker installs the sniffer to allow her to gather account names and passwords of users employing non-encrypting services, such as telnet, ftp, and POP or IMAP email accesses. A typical sniffer log contains information like this:

```
fastppp107.idirect.com => hacked.site [23]
!'"#P 38400,38400'LINUXhacked
EK!@#$$%^
ls
cd ...
ls -lat tcp.log
pico tcp.log

----- [Timed Out]
```

```
fastppp107.idirect.com => hacked.site [21]
USER hacked
PASS EK!@#$%^
TYPE I
CWD qcrack101
PORT 207,136,97,107,4,172
STOR passwd.genesis3
```

----- [Timed Out]

```
trt-on19-26.netcom.ca => hacked.site [23]
!'"#P 38400,38400'LINUXhacked
EK!@#$%^
$
hacked
EK!@#$%^
telnet grads2.phhys.cwru.edu
```

----- [Timed Out]

```
glibm10.cen.uiuc.edu => hacked.site [21]
USER hacked
PASS EK!@#$%^
TYPE I
CWD ...
PORT 130,126,160,140,16,109
TYPE A N
NLST tcp.log
TYPE I
PORT 130,126,160,140,16,110
RETR tcp.log
QUIT
```

----- [FIN]

This sniffer log shows no times for login sessions, but it does show account names and passwords, as well as commands typed (all content of electronic communications, and all captured in real-time.) Of course in this example it is the attacker who logged *her own communications*, exposing her stepping stones, the act of viewing and copying the sniffer log files ("tcp.log"), and kindly noting where these files may be found. All of this information, if provided to law enforcement at an early enough stage, would allow them to execute search warrants and subpoenas for the "evidence, instrumentalities, or fruits of crime."

The most problematic point at which real-time interception of content of communications occurs is the interception of IRC chat that is relayed through the compromised computer. This is the point at which we sail out into uncharted legal waters, where courts have not ruled on these issues. In an essay by Orin Kerr, the law here creates a "bizarre result," in which a "computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims."¹⁰ What Mr. Kerr points out is that because the law does not differentiate between authorized and unauthorized communications (i.e., it appears to protect *all electronic communication* to the same degree), the investigator trying to determine what kind of unauthorized activity is occurring on their systems and network, *may be violating the privacy rights* of those who perpetrated the intrusion. Or they may be violating the rights of third parties who are communicating over IRC channels installed on someone else's network and computer resources.

Access to stored communications

In the last section, where the attacker's own keystrokes were logged (and the location of sniffer logs was discovered) and handed over to law enforcement, the actual logs themselves have now become stored electronic communications. If law enforcement wanted to access these files to prove that computer trespass had occurred, it would necessitate issuance of a 18 USC § 2703(c) search warrant. This is the section of the ECPA that allows law enforcement to access stored electronic communications.

The investigator who analyzed a bit-image copy of the compromised computer's hard drive was also accessing stored electronic communications. It may not seem as such, but the law defines any transfer of electronic data from one system to another as an electronic communication. One party to this communication is our attacker, who sent files (for example the sniffer and Trojan horse SSH daemon and root kit files) to the compromised computer. The other party to the communication was (indirectly) the owner of the system, since the files were transferred to that person's computer.

So if the intruder initiated a communication to the compromised system, does she have a right to privacy in the contents of those files? The courts have ruled "no" on this issue. There is case law to show that privacy rights are lost when there is no legitimate expectation of privacy because of insufficient means of or authorization to protect access to material.¹¹

Disclosure of communications

Communications which are obtained legally by a private party may be legally disclosed to anyone the private party chooses.

Victims of crimes are free to disclose information about those crimes to law enforcement, without necessitating a warrant or subpoena. If you are not the victim, but instead provide services to someone suspected of involvement in a crime, transactional records and stored communications related to the suspect may *not* be disclosed to law enforcement without proper warrants, court orders, or subpoenas.

In our scenario above, the sniffer logs (real-time interception of content of communication) and files placed on the system (stored communications in which the attacker has no ownership or privacy rights) may be freely given to law enforcement without warrants, court orders, or subpoenas.

Disclosure of stored electronic communications also occurs when our intruder copies files from the compromised system, including sniffer logs that show login account names and passwords, and gives them to someone else (e.g., trades shell accounts for stolen credit cards, unpublished exploit programs -- also known as "zero day" exploits, because they have been known publicly for zero days -- or pirated software programs), or when they take someone's email inbox and publish the contents of these private communications on the Internet.

A Honeypot Scenario

Now that we've seen how existing federal statutes apply to a typical attack/defend scenario, now let's see how a typical Honeypot scenario differs in some subtle and not so subtle ways.

(Go on to a discussion of the subtle difference between a system administrator or incident responder vs. someone who installs a honeypot strictly to observe an intruder in action. E.g., It may be necessary that there be some nexus with protection in order for someone to enjoy the exceptions provided by current privacy laws.)

Opinion

(Here is where we will state our opinion of which proposed changes in federal statutes, e.g., those made by Orin Kerr, Robert S. Steere, Julie J. McMurray, etc., make the most sense from a technical perspective. John Christensen of Preston Gates Ellis, LLC, has suggested that we take the following tack: first publish a white paper on the topic, followed by a law review article that he volunteered to help author, and finishing off with a technical journal opinion piece. Representatives of the National Security Telecommunications Advisory Committee sub-group on legislation have also expressed an interest in helping research and form an opinion piece.)

Summary

(Here is the summary)

Questions (This needs more research and to be integrated into the body.)

1. Does the honeypot need to be "providing" service sometimes for it to fall under that exception?
2. Can one be a provider to oneself? Yes, Bohach vs. City of Reno is a provider to oneself case - police paging system 932 F.Supp 1232.
3. State of Washington vs. Riley 846 P.2d 1365 - pen register case.
4. Hueneman, David Law Review article - service provider exemption stuff FIDNet p 1073-1074

5. 24 Rutgers Computer and Tech L.J.1 Katrin Schatz-Byford p. 44 Differences in expectation of privacy depending on which network service you're using
6. Does wireless traffic have same protections as cordless phones?
7. Keeping Private Email Private Robert S. Steere.
8. Equivalence of protection between real-time and stored communications, such as one between points of sender and receiver (including intermediate storage), another set for after it's been read (access to stored communications). How would these help or not help the situation?
9. Kerr, Are We Overprotecting Code article
10. Who wrote about the dangers of applying both intercept and stored to accessing something, and how the courts might interpret that as double jeopardy ("infinite" jeopardy)?
11. Christian David Hammel Shultz (Notre Dame Law Review) on Carnivore and the need to revise the pen trap, claiming it's not a trap/trace or pen register, because the definition includes attaching to a line and recording #'s, while Carnivore records emails addresses. Is our IDS a pen/trap device then?
12. Also quote from above for lack of differentiation between definitions of stored vs. real-time communications in ECPA.

Credits

This paper was based in large part on guidance provided by Jennifer Granick, Litigation Director at Stanford Law School's Center for Internet and Society, and Richard Salgado, a prosecutor in the Computer Crime and Intellectual Property Section of the United States Department of Justice (Richard's contributions are strictly his own personal efforts and do not in any way reflect the official positions of the United States Department of Justice), as well as from input from John Christensen of Preston Gates Ellis, LLC.

References

"Are We Overprotecting Code? Thoughts on First-Generation Internet Law," Orin S. Kerr, Washington & Lee Law Review, Fall 2000 [57 Wash & Lee L. Rev. 1287]

"The Electronic Communications Privacy Act: A Guide for Internet Service Providers," The Law Enforcement and Security Council, [\[URL?\]](#)

"Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment," Katrin Schatz Byford, Rutgers Computer and Technology Law Journal, 1998 [24 Rutgers Computer & Tech. L.J. 1]

"Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws," Eric J. Sinrod and William P. Reilly, Santa Clara Computer and High Technology Law Journal, May 2000 [16 Computer & High Tech. L. J. 177]

"Keeping 'Private E-Mail' Private: A Proposal to Modify the Electronic Communications Privacy Act," Robert S. Steere, Valparaiso University Law Review, Fall 1998 [33 Val. U.L. Rev. 23]

"Privacy in the Information Age: The Need for Clarity in the ECPA," Julie J. McMurray, Washington University Law Quarterly, Summer 2000 [78 Wash. U.L.Q. 597]

"The Fourth Amendment in Cyberspace: Can Encryption Create a 'Reasonable Expectation of Privacy?'," Orin S. Kerr, Connecticut Law Revue, Winter 2001 [33 Conn. L. Rev. 503] ([May not apply directly](#))

"Federal Statutes – Electronic Communications Privacy Act of 1986 – Ninth Circuit Holds That the Wiretap Act Protects Electronic Communications to the Same Extent as Those in Transit," The Harvard Law Revue Association, June 2001 [114 Harv. L. Rev. 2563]

"The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?," Stephen K. Bayens, Drake University Law Revue, 2000 [48 Drake L. Rev. 239]

"Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks," Paul Taylor, Virginia Journal of Law and Technology, Spring 2001 [6 Va. J.L. & Tech. 4]

"Symposium on Internet Privacy: At the Intersection of Visible and Invisible Worlds: United States Privacy Laws and the Internet," Santa Clara Computer and High Technology Law Revue, May 2000 [16 Computer & High Tech. L.J. 357]

"The Private Workplace and the Proposed 'Notice of Electronic Monitoring Act': Is 'Notice' Enough?," Nathan Watson, American Legal Studies Association, The Legal Studies Forum, December 2001 [54 Fed. Comm. L.J. 79]

"Privacy on Federal Civilian Computer Networks: A Fourth Amendment Analysis of the Federal Intrusion Detection Network," David Hueneman, The John Marshall Journal of Computer & Information Law, Summer 2000 [18 J. Marshal J. Computer & Info. L. 1049]

"Between Big Brother and the Bottom Line: Privacy in Cyberspace," Seth Safier, Virginia Journal of Law and Technology, Spring 2000 [5 Va. J.L. & Tech. 6]

"Concerned or Just Plain Nosy? The Consequences of Parental Wiretapping Under the Federal Wiretap Act in Light of Pollock v. Pollock," Laura S. Killian, Dickinson Law Revue, Spring 2000 [104 Dick. L. Rev. 56]

"E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute," Thomas R. Greenberg, The American University Law Revue, Fall 1994 [44 Am. U.L. Rev. 219]

"Unrestricted Federal Agent: 'Carnivore' and the Need to Revise the Pen Register Statute," Christian David Hammel Schultz, Notre Dame Law Revue, June 2001 [76 Notre Dame L. Rev. 1215]

"Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001," CCIPS [\[URL?\]](#)

"The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet," March 2000 [\[URL?\]](#)

Appendix A - The Laws

A good website to read the text of US Federal laws is Cornell and The Legal Information Institute's Code Collection.¹² Make sure you are looking at the most updated version of the code. Included here are sections pertinent to this discussion only.

Computer Fraud and Abuse Act (CFAA) – 18 USCS § 1030

The CFAA deals with fraud and related activity in connection with computers. This is considered the primary federal anti-hacking statute.¹³ Some selected subsections state:

(a) Whoever--

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$ 5,000 in any 1-year period;

(5) (A) (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$ 5,000 in value;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Many of the other sections in the CFAA deal with computers used by the government, and health-related or financial institutions. If you are administering a system used - even in part - by the government, hospital, or a bank, you should explore those sections further.

Electronic Communications and Privacy Act (ECPA)

The ECPA was enacted in 1986 to update out-of-date legislation that dealt with invasion of privacy through electronic surveillance. It refers to two different types of computing service providers; "electronic communication services" and "remote computing services." The ECPA enacted and amended legislation in multiple parts of United States Code, Title 18.¹⁴ Of these, the most important to us are changes it made to the Wiretap, Stored Communications, and Pen/Trap Acts.

Wire and Electronic Communications Interception and Interception of Oral Communications (Wiretap) – 18 USCS § 2510

The Wiretap Act deals with the content of real-time communications. Some selected subsections state:

(1) Except as otherwise specifically provided in this chapter [18 USCS §§ 2510 et seq.] any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic

communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections **2511(2)(a)(ii)**, **2511(2)(b)-(c)**, **2511(2)(e)**, 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a) (i) It shall not be unlawful under this chapter [**18 USCS §§ 2510 et seq.**] for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(d) It shall not be unlawful under this chapter [**18 USCS §§ 2510 et seq.**] for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(g) It shall not be unlawful under this chapter [**18 USCS §§ 2510 et seq.**] or chapter 121 of this title [**18 USCS §§ 2701 et seq.**] for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter [**18 USCS §§ 2510 et seq.**]--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title) [**18 USCS §§ 3121 et seq.**]; or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(3)

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

(i) as otherwise authorized in section **2511(2)(a)** or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;

or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

For the purposes of a Honeynet, the most important subsection is probably the one that provides exceptions for service providers (subsection 2). Some of the language here is very specific; these selected definitions are taken from the most recent version (post USA Patriot Act) of 18 USCS § 2510.

As used in this chapter [**18 USCS §§ 2510 et seq.**]--

(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;

(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;

(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.

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(13) "user" means any person or entity who--

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means 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;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(17) "electronic storage" means--

(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;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

If you are "acting under color of law," (you are law enforcement or you are working with law enforcement) you definitely need to read the whole statute. There are several guides for law enforcement that go into much greater detail about the methods and restrictions to be used when monitoring oral, wire, or electronic communication. One of these is [Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations \(January 2001\)](#), published by the Department of Justice.¹⁵

If you are working for an Internet Service Provider, read *The Electronic Communications Privacy Act: A Guide for Internet Service Providers*, published by the Internet Alliance.¹⁶ It is similar to *Seizing Computers*, above, but aimed at service provider professionals.

Stored Wire and Electronic Communications and Transactional Records Access – 18 USCS § 2701

This section of code deals exclusively with stored communications.

§ 2701. Unlawful access to stored communications

(a) Offense. Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(1)

(c) Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user.

§ 2711. Definitions for chapter

As used in this chapter [18 USCS §§ 2701 et seq.]--

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system; and

Clearly, the person monitoring communications under protection of this statute needs to fit the definition of electronic communication service, given in 18 USCS § 2510(15), above. Also, "any company or government entity that provides others with means of communicating electronically can be a 'provider of electronic communications service' relating to the communications it provides, even if providing communications service is merely incidental to the provider's primary function. Conversely, a service cannot provide ECS with respect to a communication if the service did not provide the ability to send or receive that communication."¹⁷

Note that the term "remote computing service" is by definition a service to the public. Thus, a university is probably not a remote computing service. However, there are situations where a provider is considered an electronic communication service provider with respect to one communication, and a remote computing service with respect to another.

Pen Registers and Trap and Trace Devices (Pen/Trap) – 18 USCS § 3121

The Pen/Trap deals with transactional electronic communications, and prohibits pen register and trap and trace device use, with exceptions.

(a) In general. Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception. The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

Once again, the relevant subsection for Honeynets is the one providing electronic service providers legal ability to monitor transactional communications. The following definitions for this section come from 18 USCS § 3127.

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;

(3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

The Patriot Act

The USA Patriot Act (October 2001) affects law enforcement for the most part. It resulted in a number of changes to Federal statutes governing the searching and seizing of computers and the gathering of electronic evidence. The Department of Justice updated their *Seizing Computers* document for changes enacted by the Patriot Act in [Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001](#).¹⁸

Although criticized by some privacy groups, the Patriot Act does close a strange loophole created by lack of clarity in previous Wiretap language. The Wiretap Act allows computer owners to monitor activity on their computers. That

communication falls under the definition of "wire or electronic communication." Until the Patriot Act was passed (and the Wiretap Act updated), law enforcement was not explicitly allowed to help computer owners catch suspected hackers, because that would mean law enforcement was monitoring protected communications.

¹ For a recent case involving the use of banners in a university setting, see *United States v. Angevine*, No. 01-6097, United States Court Of Appeals For The Tenth Circuit, 2002 U.S. App. LEXIS 2746, 2002.

² Definition of electronic communications service from 18 USC § 2510 (15): "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.

Definition of remote computing service from 18 USC § 2711 (2): "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

³ Kerr, Orin S. *Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Computer Crime and Intellectual Property Section (CCIPS), United States Department of Justice, January 2001. <<http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm>>

⁴ See *Bohach v. City Of Reno*, Cv-N-96-403-Ecr, United States District Court For The District Of Nevada, 932 F. Supp. 1232; 1996 U.S. Dist. LEXIS 10715; 11 BNA IER CAS 1707, 1996.

⁵ See Kerr, *supra* note 3.

⁶ See *State Wide Photocopy v. Tokai Fin. Servs. Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995). (Financing company that used fax machines and computers but did not provide the ability to send or receive communications was not a provider of electronic communication service).

⁷ See *United States v. Seidlitz*, 589 F.2d 152, 158 (4th Cir. 1978), and *United States v. Mullins*, 992 F.2d 1472 (9th Cir. 1993).

⁸ See 846 P.2d 1365. Computer Trespass: Revised Code of Washington 9A.52.110.

⁹ Honeynet Project reference analysis of compromised host: <<http://project.honeynet.org/challenge/results/dittrich/evidence.txt>>

¹⁰ Kerr, Orin S., *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

¹¹ See *United States v. Poulsen*, No. 94-10020, United States Court Of Appeals For The Ninth Circuit, 41 F.3d 1330; 1994 U.S. App. LEXIS 34238; 94 Cal. Daily Op. Service 9349; 94 Daily Journal DAR 17306.

¹² <<http://www4.law.cornell.edu/uscode>> All of the laws discussed appear in United States Code, Title 18, Parts I and II.

¹³ See Eric J. Sinrod and William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Computer & High Tech. L.J. 177 (2000). This paper details many different hacking scenarios where 18 USC § 1030 can be applied.

¹⁴ The ECPA amended, among other laws, 18 USC §§ 2510-2522, and created 18 USC §§ 2701-2711 and 18 USC §§ 3121-3126. The term ECPA is often used to refer collectively to 18 USC §§ 2510-2522 and 18 USC §§ 2701-2711. The term "Title III" is generally used to refer specifically to 18 USC §§ 2510-2522.

¹⁵ See Kerr, *supra* note 3.

¹⁶ <<http://www.internetalliance.org>>

¹⁷ See Kerr, *supra* note 3.

¹⁸ *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*. Computer Crime and Intellectual Property Section (CCIPS), United States Department of Justice. <<http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm>>