8 Legal Issues

Richard Salgado

The views expressed in this chapter are those of Richard Salgado and do not necessarily represent the views of the Department of Justice.

Identifying the right technical configurations is only part of the job of designing and deploying a honeynet. There are also legal issues that you need to consider to reduce the risk that you will find yourself embroiled in litigation or otherwise entangled with the legal system. Failing to address these properly can make your honeynet an expensive liability. Forethought can go a long way to avoiding these legal pitfalls, and with an understanding of the relevant laws, you can take steps to reduce your exposure.

In this chapter, I will first address the limitations imposed on network operators who would like to monitor the activities of system users. The law in this area is developing, and there are discernible rules that may be surprising to lawyers and nonlawyers alike. Second, I address the possibility that your honeynet will detect improper activity, discuss what types of conduct are criminal in the U.S., and describe protocols that may be helpful in the event your honeynet becomes a witness to a crime. Third, I discuss the possibility of liability for running a honeynet that injures others.

The bottom line for the entire discussion is that you should consult with your lawyer before you design or deploy your honeynet. If you are considering a honeynet for your organization, check with counsel who advises the organization. In the case of a large enterprise, there may be in-house counsel who can provide the necessary guidance; if not, your enterprise may need to consult with outside counsel. For government agencies, there may be an office of general counsel, Inspector General, or other source of advice. (Government organizations in the U.S. may also consult with the Computer Crime and Intellectual Property Section in the Department of Justice for guidance.) Your counsel will take into account your particular situation and goals, the regulations, state law, and local law applicable to you, and will help you identify potential problems and solutions.

Many of the concerns I discuss here apply equally to computer networks generally, even those that are not honeynets.

MONITORING NETWORK USERS

The first point is one that often surprises many people: Just because you own and are responsible for a computer network does not mean that you have unfettered legal authority to monitor users of the network, even if your network is a honeynet populated exclusively by intruders. There are many possible sources of restrictions that could make monitoring improper (such as statutes, internal policies, and user agreements). Failing to honor these restrictions could land you in civil and even criminal hot water. In the honeynet context, these rules take on particular significance because the entire value of the honeynet may be tied to monitoring. I first address the potential restrictions found in the U.S. Constitution and federal statutes.

U.S. CONSTITUTIONAL PROVISIONS

If your honeynet is operated at the direction of the government, consider the (unlikely) possibility that the Fourth Amendment to the U.S. Constitution could apply. The Fourth Amendment limits the power of government agents to search for evidence without having first secured a search warrant from a judge. Evidence seized in violation of the Fourth Amendment may not be admissible at a criminal

trial against the person who was subjected to the illegal search. In addition, the person who violated the Fourth Amendment rights of another may be subject to a lawsuit for money damages.

The Fourth Amendment applies only where the person searched has a "reasonable expectation of privacy." Those who hack into networks do not have a "reasonable" expectation of privacy in their use of the victim network.[1] In addition, the Fourth Amendment restricts searches only by the government; a private actor may deploy a honeynet and monitor users without worrying about the Fourth Amendment, unless the private actor is an instrument or agent of the government.[2] Similar provisions in state constitutions are at least as rigorous as the federal Constitution, and perhaps more.

Think about whether your organization is subject to the Fourth Amendment; you might be surprised to discover that your organization is a government entity for the purpose of the amendment. For example, because of their research value, academics and students may be drawn to the idea of deploying honeynets with an eye toward studying the results. If the honeynet is deployed in connection with a *public* university, the rules of the Fourth Amendment may well apply to the monitoring. Of course, as I noted above, a honeynet that monitors only the activities of intruders will not violate the Fourth Amendment because intruders do not have a reasonable expectation of privacy. If the scope of the monitoring goes beyond the intruders, however, the Fourth Amendment issue may be very real.

U.S. STATUTES

In the U.S., there are privacy laws that can apply to the operation of a honeynet. The two federal statutes most worthy of discussion here are the Wiretap Act and the awkwardly named Pen Register, Trap and Trace Devices statute. The Wiretap

1. *U.S. v. Seidlitz,* 589 F.2d 152, 160 (4th Cir. 1978) ("having been 'caught with his hand in the cookie jar,'" hacker has no constitutional right to suppression of evidence gathered from victim computer); see *Rakas v. Illinois,* 439 U.S. 128, 143 n.12 (1978) (burglar has no reasonable expectation of privacy while on victim premises); *Compuserve, Inc. v. Cyber Promotions, Inc.,* 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (courts have likened computer hacking and trespassing).
2. *U.S. v. Jacobson,* 466 U.S. 109, 115 (1984).

Act covers the interception of the contents of communications. The Pen Register, Trap and Trace Devices statute covers the collection of noncontent information. This is not an easy area of the law, but the penalties for violation can be severe. Do not ignore these rules.

The Wiretap Act

The federal Wiretap Act generally forbids the interception of the content of communications (including electronic communications) unless one of the exceptions listed in the statute applies. Sniffing traffic on a network may be considered an interception of electronic communications and would fall within the scope of the Wiretap Act.[3] A violation of the Wiretap Act is no small matter. It can lead to a civil suit and may constitute a federal felony punishable by a fine and up to five years in prison.[4]

If your honeynet is not configured to capture the content of communications of users, then there is no Wiretap Act issue.[5] Thus, for example, if you operate a low-interaction honeynet, you may have it configured to log only the IP addresses and port calls of incoming connection attempts. If so, then the honeynet is acquiring only communications-related data, but not the content of any communications themselves. The Wiretap Act would not apply (although the Pen Register, Trap and Trace Devices statute may).

---

3. In re *Pharmatrak, Inc. Privacy Litig'n,* No. CIV.A.00-11672-JLT, 2002 WL 1880387 (D. Mass., Aug. 13, 2002); In re *DoubleClick Inc. Privacy Litig'n,* 154 F.Supp.2d 497 (S.D.N.Y. 2001).
4. 18 U.S.C. § 2511(4) & (5).
5. In the course of running a honeynet, you may find that users are uploading data to the honeynet. An intruder may, for example, set up file transfer protocol ("FTP") services and store files for later retrieval. Looking at those stored files probably would not implicate the Wiretap Act, because there would be no interception of the communications in transit. Accessing the stored communications of users may implicate the stored communication portion of the Electronic Communications Privacy Act (ECPA). ECPA creates privacy rights for customers and subscribers of certain computer network service providers. 18 U.S.C. §§ 2701–2712. For a comprehensive, but accessible, discussion of those rules, see "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" published by the Computer Crime and Intellectual Property Section of the U.S. Department of Justice (*http://www.cybercrime.gov/searching.html*).

As a constitutional matter, an intruder has no reasonable expectation of privacy while in your network. This does not mean, however, that monitoring is allowed under the Wiretap Act. Strange as it may seem, a hacker may have no reasonable expectation of privacy under the Constitution, but may nonetheless have privacy rights under the Wiretap Act.

The Wiretap Act contains many exceptions to the prohibition against intercepting the contents of communications. With regard to honeynets and other computer systems, exceptions to consider include the "provider protection" exception and the "consent of a party" exception. If monitoring is done by the government, the "computer trespasser" exception may also apply.

The Provider Protection Exception The "provider protection" exception allows an electronic communication service provider to intercept communications to protect the provider's rights or property.[6] Providers can monitor communications over their system to prevent, for example, abuse or damage to the system. This exception allows network operators to monitor hostile activity, run intrusion detection software, and scan the contents of inbound traffic for malcode signatures without violating the Wiretap Act.

The exception states:

> It shall not be unlawful under [the Wiretap Act] 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.[7]

6. 18 U.S.C. § 2511(2)(a)(i).
7. 18 U.S.C. § 2511(2)(a)(i).

Under this exception, providers may listen and record communications to prevent against fraud, theft of services, damage, and privacy invasions, for example. Even if the monitoring is done to assist law enforcement to pursue a criminal investigation, the exception is proper if it serves to protect the provider's rights or property.[8]

This is not an unlimited exception, however. Providers must balance the need to protect their rights and property with the privacy needs of the legitimate users of the services. Monitoring is permitted under the Wiretap Act if there is a "substantial nexus" between the monitoring done and the threat to the provider's rights or property.[9] Where the monitoring is done for other purposes, it will fall outside the exception and may violate the Wiretap Act if no other exception applies. This was the situation a cellular phone provider found itself in when assisting the police to investigate a kidnapper. The kidnapper had made calls from a cloned cell phone, and the police asked the cell phone company to intercept communications in the hopes of learning who the kidnapper was, and finding the victim. The company agreed and listened to calls to and from the cloned phone. From the intercepted calls, the police were able to find and arrest the kidnapper. Amazingly, the kidnapper then sued the police for violating the Wiretap Act, arguing that the provider protection exception did not apply to the interception. The trial court agreed. The court found that the exception did not apply because the phone company was not intercepting to protect its rights or property (for example, preventing theft of services); it was done to advance the interest of the police in investigating the kidnapping.[10]

The courts have not addressed whether the provider protection exception applies to interceptions of communications to or from a honeynet. There is some tension between the claim that sniffing traffic on a honeynet is done to protect the rights or property of the honeynet operator and the fact that the honeynet is deployed for the very purpose of being attacked. Arguably, sniffing on a honeynet

8. See *U.S. v. Harvey,* 540 F.2d 1345, 1352 (8th Cir. 1976).
9. See *U.S. v. Auler,* 539 F.2d 642, 646 (7th Cir. 1976) (telephone company); *United States v. Harvey,* 540 F.2d 1345, 1350 (8th Cir. 1976); *United States v. Freeman,* 524 F.2d 337, 340 (7th Cir. 1975); *United States v. McLaren,* 957 F. Supp. 215, 219 (M.D. Fla. 1997).
10. *McClelland v. McGrath,* 31 F. Supp. 2d 616 (N.D. Ill. 1998).

is not done by the provider to protect the honeynet; rather, the honeynet is there to give the provider something to sniff.

This is not to say that the provider protection exception would never apply; the courts simply have not yet addressed the issue, and there is a risk that the courts will reject its application. So how can you deal with this risk? First, certain honeynet configurations may give you a better argument that the exception applies than do other configurations. By carefully planning your configuration, you may be able to strengthen your argument that the honeynet has a role in protecting other parts of your network. (I address examples of such configurations below.) Second, whatever configuration you ultimately deploy, take the time to document the protective purposes of the honeynet. If called on later to prove that the exception applies, you will find that documentation very useful to support your argument that the purpose of the honeynet was to protect other servers.

The bigger the role a honeynet plays in protecting a production server or network, the better the chance that the provider protection exception will apply. Below are five examples of honeynets, each of which may be viewed differently by a court based on its value in protecting a production server.

- **Example 1: Independent from Production Server** In this scenario, the honeynet is unrelated to any particular production server, as shown in Figure 8-1. The most that can be said about the protective value of this honeynet is that it may, in a long-term and somewhat abstract sense, protect production servers across the Internet by generally enhancing the art of network attack detection, prevention, and response.

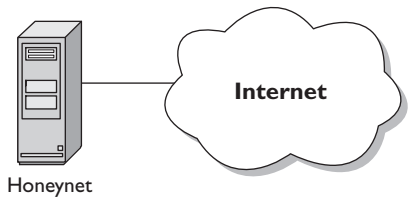

Figure 8-1 This honeynet is unrelated to any particular production server.

■ **Example 2: Configuration-Dependent** In this scenario, the honeynet is configured identically, in material respects, to a particular production server of the honeynet operator, as shown in Figure 8-2. It may run the same operating system, use the same hardware, run the same services, use the same firewall and signatures, or be identical in other ways to a particular production server. The honeynet is not, however, connected in the same subnet as the production server. The goal of this honeynet may be to secure a production server (or class of production servers) operated by the honeynet owner by (a) revealing the attacks (and perhaps identifying the signatures of the attacks) that are directed at the particular configuration, (b) revealing vulnerabilities that exist in that configuration, and (c) making it easier to develop and test response tactics to limit the effectiveness of the attacks.

If sued for a federal Wiretap Act violation for sniffing traffic on the honeynet, the operator of this honeynet may be able to argue that the provider protection exception allowed for the monitoring because it led to enhanced security measures for the operator's production servers. If the honeynet operator has documented that this was a goal of the honeynet from the outset, and has documented the security improvements implemented on the production servers that were developed as a result of lessons learned from the honeynet monitoring, the operator has increased the chance that a court will agree that the exception applies.

■ **Example 3: IP Address-Dependent** In this scenario, the honeynet is nestled within a contiguous IP address range used by production servers of the honeynet operator, as shown in Figure 8-3. Scans of the IP address range will cover the production servers as well as the honeynet. The honeynet can be configured

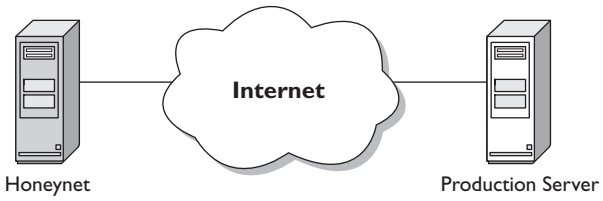

Figure 8-2 This honeynet is configured identically, in material respects, to a particular production server of the honeynet operator.

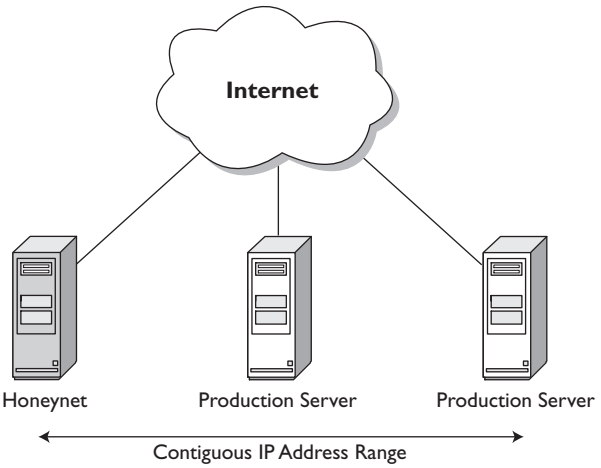

Figure 8-3 This honeynet is nestled within a contiguous IP address range used by production servers of the honeynet operator.

to appear identical, in material respects, to one or more of its production server neighbors on the network. The goal of the honeynet operator may be to secure his or her production neighbors by (a) revealing the attacks (and perhaps identifying the signatures of the attacks) that are directed at the configuration used by the production servers, (b) revealing vulnerabilities that exist in that configuration, and (c) making it easier to develop and test response tactics to limit the effectiveness of the attacks.

In addition, the honeynet could be configured to be vulnerable to particular types of attacks and populated with tantalizing data. The attention of a would-be attacker who scans the IP address block for vulnerable computers may be drawn to the honeynet and away from the relatively secure production servers. The honeynet protects the production servers, the operator may argue, by acting as a lightning rod for attacks that would have otherwise hit the production servers.

■ **Example 4: Demilitarized Zone** In this scenario, the honeynet is located behind a firewall in the so-called demilitarized zone (DMZ) with production servers such as mail or web servers, but separate from the rest of the internal network, as shown in Figure 8-4. The honeynet could be listening to the ports

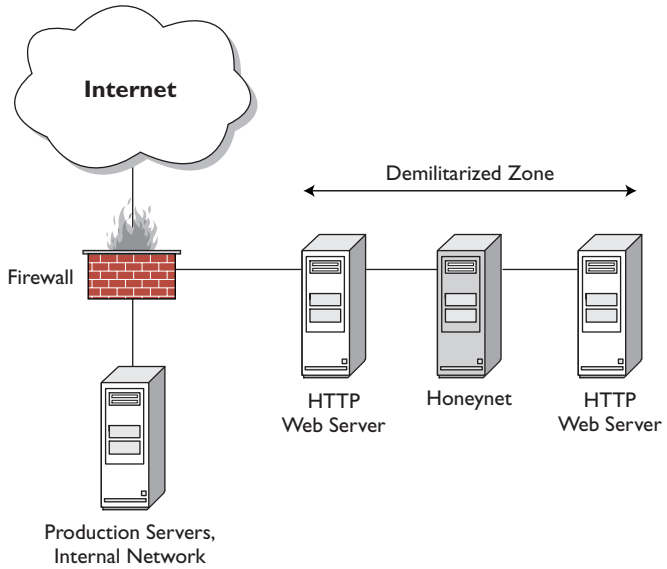

Figure 8-4 This honeynet is located behind a firewall in the so-called "DMZ" with production servers such as mail or web servers, but separate from the rest of the internal network.

served by the other servers in the DMZ. Any connections to those ports would be presumed attacks, and likely attacks that are also being launched against the other servers. Unlike the other servers, however, the honeynet may be taken down and analyzed without disrupting services offered to legitimate users. This enhances the organization's ability to identify attacks that are in all likelihood also being directed at the other DMZ servers, identifying vulnerabilities that exist in those servers, and finding means to prevent and respond to the attacks. The honeynet operator could argue that the honeynet protects the servers in the DMZ by acting as an attack lightning rod, and also serves to identify attacks that may be intended for the internal production servers.

■ **Example 5: Sandbox** In this scenario, the honeynet is actually part of the production server, as shown in Figure 8-5. It is also referred to as a "sandbox." The software Back Officer Friendly by NFR Security, Inc. is a simple example of this approach. The sandbox honeynet sees attacks or attempted attacks against the very production server on which the honeynet is running. The sandbox,

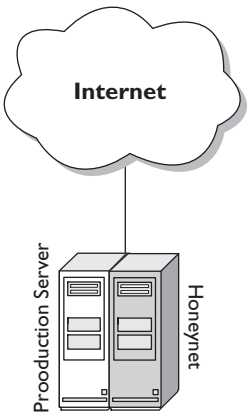

Figure 8-5 This honeynet is actually part of the production server. Such honeynets are also at times referred to as "sandboxes."

compared with the other types of honeynets, plays a relatively immediate role in the protection of the production server. The honeynet operator could argue that the honeynet, intimately associated with the production server, plays a direct role in preventing attacks against the production server.

The Consent of a Party Exception The "consent of a party" exception is fairly intuitive.[11] If a party to a communication has consented to monitoring (or if a party actually does the intercepting), the interception is permitted under the Wiretap Act (unless it was done for some other unlawful purpose). A honeynet operator may be able to get consent from attackers by placing a "consent banner" on the honeynet. The banner would tell users (including would-be attackers) that by accessing the system they are consenting to monitoring. If a hacker uses the system having seen the banner, the hacker has assented to the terms and given the system operator consent to monitor the session.

In addition, arguably when an intruder communicates with the honeynet (for example by uploading a file), the honeynet itself is a party to the communication

11. 18 U.S.C. § 2511(2)(c)–(d).

and can consent to monitoring.[12] This interpretation of the consent exception runs into difficulty, however, when the attacker uses the computer as a hop-through to connect with another computer. For example, if the attacker connects to a honeynet, then uses the bandwidth of the honeynet to connect with another victim computer, the honeynet stops looking so much like a party to the communication with the attacker and more like a switch between the attacker and the other victim. A honeynet operator could eliminate this possibility of being used as a hop-through by logging attempted outbound connections but blocking them and instead returning a failure reply to the attacker. There is a price to be paid by such a configuration: The honeynet may look less "real" and may be less attractive to the attackers of interest.

The Computer Trespasser Exception The "computer trespasser" exception, enacted as part of the USA PATRIOT Act, allows the government to monitor hackers in certain situations.[13] It applies where the user being monitored is a trespasser and the communications monitored are relevant to an ongoing investigation. Government must, of course, secure permission of the owner or operator of the network before monitoring. This exception may be useful for honeynet owners, particularly when the honeynet is run with a government entity.

The Pen Register, Trap and Trace Devices Statute

The Pen Register, Trap and Trace Devices statute (Pen/Trap statute) governs the real-time collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone or the destination or source IP address of a computer network user (data the statute refers to as "dialing, routing, addressing, or signaling information").[14] Like the Wiretap Act's prohibition on interception of the contents of communications, the Pen/Trap statute creates a general prohibition on the real-time monitoring of traffic data relating to communications. A pen register is a device or process that records outgoing connection information (for example, the telephone number

12. *U.S. v. Mullins,* 992 F.2d 1472, 1478 (9th Cir. 1993); *U.S. v. Seidlitz,* 589 F.2d 152, 158 (4th Cir. 1978); *In re DoubleClick Inc. Privacy Litig'n,* 154 F.Supp.2d 497 (S.D.N.Y. 2001).
13. 18 U.S.C. § 2511(2)(i).
14. 18 U.S.C. §§ 3121–3127.

dialed from a monitored telephone); a trap and trace device captures incoming connection information (for example, the phone number of a call to the monitored telephone).

The Pen Register, Trap and Trace Devices statute generally forbids the acquisition of noncontent information of a communication, unless one of the listed exceptions applies. In the computer network context, this includes, for example, network routing information, such as the source and destination IP address, the port number that handled that communication, and email addresses of the attackers. If the device or process is intended to capture content of communications, such as the subject line or body of an email or the content of a downloaded file, then its use is governed by the Wiretap Act, not the Pen Register, Trap and Trace Devices statute.

Through the Pen Register, Trap and Trace Devices statute, Congress gives network operators plenty of authority to use Pen/Trap devices on their networks. The statute has never been tested in court, however, as applied to honeynets. Providers are permitted to use Pen/Trap devices as follows:

- 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
- 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
- Where the consent of the user of that service has been obtained[15]

Notice that these exceptions follow the exceptions in the Wiretap Act. Generally speaking, if a honeynet operator fits within one of the exceptions to the Wiretap Act for intercepting the contents of communications, the operator is also authorized to intercept the noncontent information concerning the communication.

15. 18 U.S.C. § 3121(b).

Like a Wiretap Act violation, violation of the Pen Register, Trap and Trace Devices statute is a crime. Violations are punishable by a fine and up to a year in prison.[16] Treat the matter seriously, and consult with counsel.

U.S. CONTRACTS AND POLICIES

Another source of privacy rights in the U.S. for users may be contract and policies. An organization that has promised users that it will not engage in certain types of network monitoring may find itself in a lawsuit if it breaks such a promise. If your honeynet is deployed on part of a network that is subject to such monitoring contracts or policies, take care that you take them into account.

LAWS OUTSIDE THE U.S.

Countries other than the U.S. also have laws that apply to the operation of honeynets. A complete catalog of all these laws of all the jurisdictions in all the countries is well beyond the scope of this chapter. Consult counsel who knows the laws in the jurisdiction in which you plan to deploy your honeynet.

CRIME AND THE HONEYNET

Intruders on your honeynet may have nasty plans for you. Not only may an attacker intend to victimize you, the attacker may want to use your system as a launching point to attack others with your bandwidth. The attacker may want to stash contraband, such as stolen credit cards, password files, or trade secrets; perhaps the attacker will try to set up a "warez" site to traffic in pirated software or entertainment media, or use your system to distribute child pornography. Don't let your honeynet become part of the problem. Below I discuss some of the types of illicit conduct that you may see on your honeynet that could form the basis for criminal or civil action against the attacker, and provide some ideas on how to deal with evidence you collect. Before you take your honeynet live, have a plan in place for dealing with criminal conduct that your honeynet may witness.

16. 18 U.S.C. § 3121(d).

COMMON TYPES OF CRIMINAL ACTIVITY

There is a myriad of conduct that you may see on your honeynet that constitutes or evinces one or more crimes under U.S. law and that could lead to a civil lawsuit against the attacker. The most obvious crime you may expect is a network intrusion (or attempted network intrusion). There are other crimes that you may detect in the course of operating a honeynet, however. I deal with only a few here. Again, it is a good idea to consult with an attorney before and while you operate your honeynet. For many of the crimes you may see, you will want to be able to respond quickly and responsibly.

Network Crimes

In the U.S., most of the computer network crimes are defined in the federal Computer Fraud and Abuse Act.[17] I concentrate on this statute, although there are others that can apply as well, depending on the facts. In addition, most states in the U.S. have computer-crime laws that criminalize unauthorized access or damage to a computer or network.[18] The laws of other countries vary widely, but many make intrusions and network attacks criminal.[19]

The Computer Fraud and Abuse Act criminalizes certain attacks against certain computers by certain actors. Although there are many sections and subsections in the statute that cover many different types of attacks, there are a set of provisions commonly applied to most network attacks. These provisions cover so-called "protected computers."

A "protected computer" includes any computer "used in interstate or foreign commerce or communication." Basically, any computer on the Internet is "protected" under the statute because it is used in interstate communication. In

17. The Computer Fraud and Abuse Act is found at 18 U.S.C. § 1030. The text of the statute and examples of cases prosecuted under that statute can be found at *http://www.cybercrime.gov*.
18. For a partial list of state computer crime laws see *http://nsi.org/Library/Compsec/computerlaw/statelaws.html*.
19. For a partial list of computer crime laws of jurisdictions outside the U.S. see *http://www.mossbyrett.of.no/info/legal.html*.

addition, all U.S. government computers, and those used by banks and other financial institutions, are considered "protected" under the statute.[20] Computers outside the U.S. can also be "protected" under the statute.[21] This means that it can be criminal for an attacker located in the U.S. to victimize a computer located outside the U.S. (It also allows U.S. law enforcement to provide faster and easier assistance to foreign investigators when a hacker uses a U.S.-located computer as a pass-through to attack computers located outside the U.S.)

The bottom line is that for the purpose of the federal computer crime law, most honeynets are going to qualify as "protected" computers. I next discuss what protected computers are "protected" against.

Denial of Service Attacks and Malicious Code If a protected computer is the victim of a denial of service (DoS) attack or virus, worm, or other malcode with a damaging payload, the attacker may be guilty of a felony violation of the Computer Fraud and Abuse Act. It would not matter whether the perpetrator was an outside attacker who had no right to access the computer, or an inside employee, subscriber, customer, or contractor who had some legitimate right to be on the victim system. Nor is it necessary that the attacker actually gain some level of user privileges to the computer. If an attacker "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," the attacker has committed a felony violation of the law.[22] The maximum penalty for first-time offenders is a fine and 10 years imprisonment. The maximum rises to a fine and 20 years imprisonment for subsequent offenses, or if the intruder knowingly or recklessly caused serious bodily injury, and life imprisonment for knowingly or recklessly causing death.[23] The attacker would also be subject to a civil suit.[24]

20. 18 U.S.C. § 1030(e)(2).
21. 18 U.S.C. § 1030(e)(2)(B).
22. 18 U.S.C. § 1030(a)(5)(A)(i).
23. 18 U.S.C. § 1030(c)(4)(A) & (C).
24. 18 U.S.C. § 1030(g) (allowing for civil suit for compensatory damages, injunctive relief and other equitable relief).

To constitute a crime, the attack has to result in "damage." Under the statute, the term "damage" means "any impairment to the integrity or availability of data, a program, a system or information."[25] By definition, a DoS attack causes damage because it impairs the availability of data, a program, a system, or information. In addition to damage, however, to constitute a felony under this section of the statute, the attack must also have resulted in one or more of the following:[26]

- Loss to one or more persons during any one-year period aggregating at least $5,000
- Modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals
- Physical injury to any person
- A threat to public health or safety
- Damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security

Thus, if an attack on a protected computer did not result in impairment of medical records, harm to a person, threat to public safety, or damage to a government entity system, then to constitute a federal crime under the particular provisions I am discussing now, the damage from the attack must have resulted in losses of at least $5,000 in a given year. (Of course, even if the threshold is not met, the conduct may be criminal under some other provision or under applicable state law.)

Any loss that is a reasonably foreseeable result of the attack or incident can count toward the $5,000 threshold. Specifically, the statute defines "loss" to include "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 other information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[27]

25. 18 U.S.C. § 1030(e)(8).
26. 18 U.S.C. § 1030(a)(5)(B).
27. 18 U.S.C. § 1030(e)(11).

In addition, in some situations, an attack on a particular protected computer may not have resulted in much loss when viewed in isolation. To meet the $5,000 threshold, law enforcement can aggregate losses resulting from a related course of conduct that occurs within a one-year period affecting several protected computers and victims. For example, if in a single 12-month period a defendant launches a DoS attack against 11 separate websites, each single website operator may have suffered not much more than $500 loss, far below the $5,000 threshold. In a criminal prosecution of the attacker for the related attacks, however, law enforcement can satisfy the $5,000 threshold by adding those individual losses, the sum of which would exceed the threshold.

Most honeynets are unlikely to have data of any real value, or to offer services to legitimate users, so it may be that most honeynet operators could not show that they suffered significant "loss" as a result of an attack on a honeynet. This does not mean that there was no crime, however. First, as I discuss in a section to follow, there may be a charge for an attempted crime. Second, even if the attack on the honeynet itself was not criminal (although it may be), the attacker may have left valuable evidence on the honeynet that would form the basis for an investigation and prosecution of the perpetrator for criminal attacks on other victim systems.

Intrusions Of course, the Computer Fraud and Abuse Act also covers actual intrusions into a protected computer. If the attacker actually cracks your honeynet and gains user privileges, and as a result causes damage, then the attacker's conduct could also constitute a federal offense (if the intrusion caused one or more of the listed harms).[28] If the damage was caused intentionally, the maximum penalty for first-time offenders is a fine and 10 years imprisonment. The maximum rises to a fine and 20 years imprisonment for subsequent offenses.[29] If the damage was caused recklessly, the maximum penalty for first-time offenders is a fine and 5 years imprisonment. The maximum rises to a fine and 20 years imprisonment for subsequent offenses.[30] If the attacker caused damages neither

28. In sum, those harms are: aggregate loss of at least $5,000 in a given year, impairment of medical records, harm to a person, threat to public health or safety, or damage to a government entity system used in administration of justice, national defense, or national security.
29. 18 U.S.C. § 1030(c)(4)(A) & (C).
30. 18 U.S.C. § 1030(c)(4)(B) & (C).

intentionally nor recklessly, and the attacker is a first-time offender, then the attacker may receive a maximum penalty of a fine and 1 year imprisonment. The maximum rises to a fine and 10 years imprisonment for subsequent offenses.[31]

Other Computer "Access" Crimes Other provisions in the Computer Fraud and Abuse Act prohibit attackers from obtaining information from government systems, financial institutions, and credit card issuers.[32]

There is a violation almost any time a hacker breaks into a computer to obtain information, even if the hacker does not damage the integrity or availability of the data. The crime is more serious if committed for commercial advantage or private financial gain, in furtherance of another crime, or if the information obtained is worth more than $5,000.[33] The maximum penalty for first-time offenders is a fine and 1 year imprisonment (a fine and 5 years imprisonment if committed with commercial or financial motives).[34] The maximum rises to a fine and 10 years imprisonment for subsequent offenses.[35]

It is also a crime under the act to access, without authorization, any nonpublic U.S. government computer, even if no information is obtained nor damage inflicted.[36] Hacking into a computer to further some fraud, and thereby gain anything of value (other than the value of computer cycles themselves), is yet another offense under the act.[37] Computer-related espionage, or obtaining classified information by means of a computer system, is also criminal under the act,[38] and may constitute a federal act of terrorism in certain circumstances.[39]

31. 18 U.S.C. § 1030(c)(2)(A) & (3)(B).
32. 18 U.S.C. § 1030(a)(1) & (2).
33. 18 U.S.C. § 1030(a)(2) & (c)(2)(B)(i)–(ii).
34. 18 U.S.C. § 1030(c)(2)(A) & (B)(i)–(iii).
35. 18 U.S.C. § 1030(c)(2)(C).
36. 18 U.S.C. § 1030(a)(3).
37. 18 U.S.C. § 1030(a)(4).
38. 18 U.S.C. § 1030(a)(1). The maximum penalty for first-time offenders of this provision is a fine and 10 year imprisonment. 18 U.S.C. § 1030(c)(1)(A). The maximum rises to a fine and 20 years for subsequent offenses. 18 U.S.C. § 1030(c)(1)(B).
39. 18 U.S.C. § 2332b(g)(5)(B)(i).

Trafficking in Passwords As a general matter, it is a crime under the statute to traffic in passwords.[40] A honeynet operator should pay particular attention if intruders use the honeynet to store files with names that resemble standard password files. That is a pretty compelling hint that the honeynet is being used to traffic in passwords in violation of the law.

Threatening Damage to a Computer Yet another provision in the Computer Fraud and Abuse Act makes it illegal to extort something of value by threatening to do harm to a protected computer.[41] The statute provides that the communication carrying the threat must have been transmitted in "interstate or foreign commerce," which in practical terms means sent through the mail, by telephone, or in an electronic communication on the Internet. For example, if someone in a chat session threatens to inflict damage to a computer (including a honeynet), intending to obtain money from the system owner, for example, that person may have committed a federal offense. Likewise, if a honeynet operator finds such a threat transmitted to or through the honeynet, the threat may constitute evidence of a crime even if it is a threat to a computer other than the honeynet.

Attempt to Commit a Network Crime The Computer Fraud and Abuse Act also criminalizes *attempts* to engage in conduct that would violate the Act.[42] This means that, although the crime was never completed, a defendant who took a substantial step toward completing the crime but was thwarted may still be charged as if the crime had been completed.

This concept is simple enough for most of the crimes under the Computer Fraud and Abuse Act, even when the victim computer is a honeynet. The crime of attempt becomes a bit more complicated, however, if the conduct the attacker was trying to complete would not be a crime unless it results in damage. For example, to charge a defendant under section 1030(a)(5)(A)(i) for intentionally launching a DoS attack against a company network, the prosecutor would have to show damage to a protected computer. If the attack did not result in damage because it

40. 18 U.S.C. § 1030(a)(6); see also 18 U.S.C. § 1029 (access device fraud).
41. 18 U.S.C. § 1030(a)(7).
42. 18 U.S.C. § 1030(b).

was unsuccessful, the defendant can still be charged with an attempt to launch a damaging DoS attack. Charging a hacker with attempt to commit a crime where damage must be shown may seem a bit odd, however, where the attacked computer is a honeynet. How is it that a honeynet operator (or a prosecutor) can show that damage or loss could have been suffered as the result of a successful attack on a *faux* production server? After all, the typical honeynet will not be populated with data of any real value, and there are unlikely to be legitimate users who are deprived of services as the result of an attack on the honeynet.

Although there is no published case law involving a defendant charged with attempting to attack a protected computer that turns out to be a honeynet, it is not unusual for a prosecutor to charge a defendant with an attempt to commit a crime that, unbeknownst to the defendant, could not have been committed successfully. For example, defendant who attempts to buy illegal drugs from an undercover police officer may be charged with an attempt to traffic in narcotics, even if the police officer did not actually have any illegal narcotics to sell.[43] Likewise, the government can engage in a sting operation to put trade secret thieves in jail without having to put real trade secrets at risk of disclosure.[44] One who shoots a corpse, believing it to be alive, can be charged with attempted murder, and one who sells sugar, believing it to be cocaine, can be charged with attempt to sell illegal drugs.[45]

It may be that even though a hacker is mistaken in believing that a honeynet was a production server chock-full of valuable information, and even if it would have been impossible for the hacker to have actually inflicted any damage or loss on the honeynet or its operators, the hacker may still be guilty of attempting to

43. See, e.g., *Giddings v. State,* 816 S.W.2d 538 (Tex.App., 1991); *U.S. v. Root,* 296 F.3d 1222, 1227 (11th Cir. 2002) (holding "that an actual minor victim is not required for an attempt conviction" under statute prohibiting enticing minor to engage in criminal sexual activity); *U.S. v. Brooklier,* 685 F.2d 1208 (9th Cir. 1982) (impossibility no defense to charge of attempting to extort money from undercover business operated by FBI).
44. *U.S. v. Yang,* 281 F.3d 534 (6th Cir. 2002); *U.S. v. Hsu,* 155 F.3d 189 (3d Cir.1998).
45. See *U.S. v. Lange,* 312 F.3d 263 (7th Cir. 2002). ("Events of this sort underlie the maxim that factual impossibility is no defense to a prosecution for attempt.")

violate the Computer Fraud and Abuse Act by taking a substantial step in committing the crime.[46]

Contraband

A honeynet operator should be ready in the event that the honeynet becomes a repository of contraband. Contraband comes in many forms. Child pornography and other obscene images, stolen trade secrets, pilfered passwords and user names, credit card numbers and account identifiers, and of course pirated software, music, and video are unfortunately common types of contraband that can flow easily over networks.

Crimes Committed by Juveniles

It may be that the crime is committed by a minor. Criminal defendants who are under 18 years of age are treated differently than those who are over 18 at the time of the criminal conduct. Generally speaking, the prosecution of juveniles is left in the first instance to the state courts with jurisdiction over the offense. A charge of juvenile delinquency can be brought against a minor in federal court, however, where the federal prosecutor certifies that: (a) The state(s) with jurisdiction declined to prosecute (or there is no state with jurisdiction), or (b) the state(s) with jurisdiction are not adequately equipped to handle the needs of juveniles, or (c) the crime is a violent felony (or one of the drug or gun offenses listed in the federal statute covering juveniles), or (d) the offense implicates a substantial federal interest warranting federal intervention.[47]

PROTOCOL FOR DEALING WITH ILLEGAL CONDUCT AND CONTRABAND

Before you take a honeynet "live," think about what you are going to do in the event you suspect that your honeynet has become the scene of a crime or con-

46. *U.S. v. Farner,* 251 F.3d 510, 513 (5th Cir. 2001). ("[T]his circuit has properly eschewed the semantical thicket of the impossibility defense in criminal attempt cases and has instead required proof of two elements: first, that the defendant acted with the kind of culpability otherwise required for the commission of the underlying substantive offense, and, second, that the defendant had engaged in conduct which constitutes a substantial step toward commission of the crime. The substantial step must be conduct which strongly corroborates the firmness of defendant's criminal attempt.")
47. Juvenile Justice and Delinquency Prevention Act, 18 U.S.C. § 5031–5042; see *U.S. v. F.S.J.,* 265 F.3d 764 (9th Cir. 2001).

tains evidence of criminal conduct. This is another topic that will be well worth your time to discuss with your lawyer.

Involve Law Enforcement

By its very nature, your honeynet will likely become a victim of or "witness" to criminal conduct. It may be necessary for you to call law enforcement if you see that there is in fact criminal conduct on your honeynet. There are laws that may require reporting certain types of crime.[48] Be prepared in advance of detecting crime.

Establish a Relationship with Law Enforcement If you are a private honeynet operator, one step that is easy and may prove invaluable is to establish a relationship with a law enforcement official who you can call if you detect illegal conduct on your honeynet. There are many avenues available to forge such relationships. The InfraGard program, run out of the Federal Bureau of Investigation, may provide a good entry point to meet federal, state, and local law enforcement in your area who have experience with computer crimes.[49] The field office of the Federal Bureau of Investigation and the U.S. Secret Service closest to you also have agents who work on high-technology crime cases.[50] In some parts of the country, there are Electronic Crimes Task Forces that can provide a great way to meet investigators with the skills to handle cyber crime.[51]

Do not overlook your state and local law enforcement either. Many nonfederal agencies have tremendous expertise in the crimes your honeynet may witness. (Note that if you operate a honeynet in close coordination with law enforcement or other government personnel, there is some chance that a court will conclude that you are an agent of the government and that the Fourth Amendment, discussed above, applies to the honeynet monitoring.)[52]

---

48. See, e.g., 42 U.S.C. § 13032 (those who provide electronic communication services to the public required to report child pornography violations to Cyber Tip Line at the National Center for Missing and Exploited Children); 18 U.S.C. § 4 (whoever, knowing of actual commission of a felony, conceals and fails to report as soon as possible may be imprisoned up to 3 years and fined).
49. *http://www.fbi.gov/contact/fo/fo.htm.*
50. *http://www.fbi.gov/contact/fo/fo.htm* and *http://www.ustreas.gov/usss/field_offices.shtml.*
51. *http://www.ectaskforce.org/Regional_Locations.htm.*
52. See *U.S. v. Jarrett,* 338 F.3d 339 (4th Cir. 2003) (using Trojan horse on defendant's computer, hacker found child pornography and turned over to law enforcement; hacker not deemed "agent of government" because "the Government did not know of, or in any way participate in, the hacker's search of [defendant's] computer at the time of that search").

When to Call Law Enforcement To be sure, not every port scan or worm infection will warrant a call to law enforcement. By the same token, you do not want your honeynet to facilitate criminal activity. If a honeynet operator does not act responsibly when it appears that the honeynet may be aiding a criminal, not only will the honeynet become part of the problem that honeynets generally are intended to solve, but there is a risk that the honeynet operator will be viewed with suspicion. More than a few defendants in child pornography cases have declared, unsuccessfully, that they collected the child pornography found on their computers as part of a "research" project or to ultimately "help" law enforcement. You do not want to play with fire; if you see contraband on your honeynet, do not let the situation go without a response and don't just delete it; get the police involved as soon as you can. Do not wait for the police to call you. As discussed above, by having a solid relationship with law enforcement in advance, the process can be much smoother.

Reduce Risk of Harm to Others

If you find that the honeynet has been compromised and may be used or is being used as an attack platform to victimize other networks, or is being used to distribute pilfered information, you will need to take action to prevent further damage. You certainly do not want to be implicated in the criminal attack on others through your inaction to secure the honeynet. A simple egress filter may do wonders in thwarting an attack. Regardless, consider reporting attempted attacks to law enforcement. Your honeynet may be the only source with records useful to trace the attacker.

Inform Victims

You may discover that the attackers on your honeynet have victimized others, some of whom may have no idea that they have been attacked. For example, you may find that an attacker has stashed on your honeynet a file with credit card numbers and account holder names. Similarly, you may find that your honeynet is being attacked from an upstream source that is very likely itself to be a victim of the hacker. Perhaps, although hopefully not, you may find that your honeynet is being used to attack other networks downstream. In these situations, consider notifying the victims.

Not only will notifying victims allow them to take steps to minimize any loss, they may be able to join the effort to catch the culprit. If you have called in law enforcement, the investigator can often handle victim notification for you. Assistance from law enforcement is particularly valuable in this regard.

Generally, federal government agents have no duty to warn actual or potential victims of activity associated with undercover operations, like honeynets, unless there is some special relationship with the victim.[53] Victim notification may be covered by internal policy, however. Government honeynet operators should not make a judgment call on this alone. They should check with counsel for the agency before deploying honeynets and again if any illegal activity is suspected.

ENTRAPMENT

Entrapment is often mentioned as a concern for honeynet owners. Entrapment is a narrow legal defense that a defendant in a criminal case may raise to escape conviction. It applies where the government acted in a manner that caused an otherwise unwilling defendant to commit the crime charged. If the defendant was predisposed to commit the crime or was not induced by the government to commit the crime, the defense will fail.[54] The government can provide an opportunity and facilities to the defendant to commit a crime; without much more, the defendant will not be heard to claim that he or she was entrapped.[55] The entrapment defense is not based on constitutional rights (unless the operation is so egregious that it "shocks the conscience"). It is really a test to determine whether the defendant had the requisite culpability (state of mind) to be criminally liable for the defendant's actions.[56]

53. *Powers v. Lightner,* 820 F.2d 818, 821–22 (7th Cir. 1987); *Georgia Cas. & Sur. Co.,* 823 F.2d 260, 262 (8th Cir. 1987); *Redmond v. U.S.,* 518 F.2d 811, 816 (7th Cir. 1975).
54. *Sherman v. U.S.,* 356 U.S. 369, 373 (1958).
55. *U.S. v. Hampton,* 425 U.S. 484, 488 (1976).
56. *U.S. v. Poehlman,* 217 F.3d 692 (9th Cir. 2000) (held defendant was entrapped).

The defense of entrapment has no application outside of the criminal process, and in any event, is unlikely to be of much use to a hacker who broke into a honeynet without significant government inducement.

DO NO HARM: LIABILITY TO OTHERS

In addition to the exposure to lawsuits that a honeynet owner faces if he or she violates the statutes discussed above, or contractual rights to privacy, there may be exposure to suits from others harmed by the honeynet. There has been much discussion, for example, about the possibility that a network operator could be sued for having poor security that resulted in an attack against other networks. So far, the discussion has remained largely academic.

Nonetheless, honeynet operators should be vigilant that their honeynets are not used to harm others. A honeynet operator who has configured the honeynet to be vulnerable to an intrusion should pay close attention to activities on the computer. One harmed by such a honeynet may have a field day in court pointing out that the operator intended (and hoped) that the honeynet would be compromised, and in fact made the job of the hacker easier by intentionally including security holes. Yet when the honeynet was exploited as planned, the plaintiff could argue, the operator allowed others to be harmed using the honeynet. (A honeynet run by federal agents, like most undercover operations, will lead to liability for harm done to innocent nontargets only if the court concludes that the government's conduct "shocks the conscience" or is in violation of the victim's constitutional or statutory rights.)[57]

There are several ways to reduce the risk that your honeynet will leave you a defendant in a civil lawsuit.

First, keep a close eye on your honeynet and take action to prevent it from harming others. It is not a fire-and-forget device. The best way to avoid a lawsuit for damage to another's system is to prevent the damage in the first

57. *Brown v. Nationsbank,* 188 F.3d 579, 591 (5th Cir. 1999).

instance. If you have included known vulnerabilities into the honeynet or have otherwise taken steps to drive hostile traffic to the honeynet such that you expect successful intrusions, consider setting up a paging or other notification system so that you will be informed immediately of activity on the honeynet. A good deal of harm to others can occur in just a few seconds, so be prepared to respond without delay. If such vigilance is not practical, consider taking the honeynet offline, or otherwise disabling it during the period that you have no way to attend to it. Make sure that your honeynet is not aiding the nefarious efforts of attackers.

Second, do not just sit on information if you can see that someone is being harmed in spite of your protective efforts. For example, even if you have limited, filtered, or altogether blocked outbound traffic so that the honeynet cannot be used directly as an attack platform, you may find that your honeynet is being used to store hacker tools that are pulled down for use in exploits. Similarly, you may detect an intruder uploading stolen information to the honeynet. Each of these situations holds the potential for a lawsuit. This is when time spent with your lawyer, and contacts with law enforcement can really pay off. Follow the plan you set forth before deploying your honeynet for dealing with criminal activity.

Third, be careful in selecting the data with which you are going to populate your honeynet. Do not populate the honeynet with contraband; it is no more legal for a honeynet operator to do so than the attackers who you hope will find their way to your honeynet.

With careful planning, attention to the legal issues, and close consolation with legal counsel, you can maximize the desired value of your honeynet while reducing both your legal exposure and the risks of harm to others.

SUMMARY

In designing and deploying a honeynet, take the time to consult with an attorney to identify and address the potential legal hazards before they ensnare you. There is no substitute for talking with your own lawyer, who can guide you through the laws that apply to your specific honeynet.

For honeynet deployments in the U.S., consider three legal issues. First, ensure that you are in compliance with the laws that restrict your right to monitor the activities of users on your system. Second, recognize and address the risk that attackers will misuse your honeynet to commit crimes, or store and distribute contraband. Third, consider the possibility that your honeynet will be used to attack other systems, and the potential liability you could face for resulting damage. Your lawyer may identify other legal issues as well. If you deploy a honeynet outside the U.S., look to the applicable laws of the jurisdiction in which you will operate. Designing and implementing your honeynet with attention to these concerns can help you stay out of legal trouble.

The next chapter provides an overview of the types of data that a honeynet may capture and the purpose and value of data analysis.