



Intelligence Gathering

DefCon X

Vic Vandal

vvandal@well.com



NECESSARY DISCLAIMER:

This talk discusses various illegal techniques and concepts.

The author does not endorse nor does he condone the execution of any of those illegal activities discussed.

ESPECIALLY the Information Warfare concepts.



Types of Intelligence Gathering

- ◆ Competitive Intelligence
- ◆ Corporate Espionage
- ◆ Information Warfare
- ◆ Personal Investigation

(*This talk is NOT about going to school to “become intelligent”, in case anyone expected that to be covered.)



Competitive Intelligence

- ◆ Relies solely on legal and ethical means to gather data, piece it together to form information, and analyze it to create intelligence for the use of decision-makers
- ◆ Over 95 percent of the information companies require to compete successfully is available in the public domain
- ◆ Helps organizations better understand their competitive environment and make sound business decisions



Corporate Espionage



Corporate Espionage

- ◆ “Espionage” - the collection, collation, and analysis of illicitly gained information
- ◆ “Corporate Espionage” - the theft of trade secrets for economic gain
- ◆ “Trade Secret” - property right which has value by providing an advantage in business over competitors who do not know the secret
- ◆ International Trade Commission estimates current annual losses to U.S. industries due to corporate espionage to be over \$70 billion



How It's Generally Done

- ◆ Over 70% of capers involve “Inside Jobs”
 - Disgruntled employees
 - Bribes from a competitor
 - Cleaning crews
 - Industrial mole
- ◆ False Pretenses
 - Companies hire a competitors employee for their trade knowledge
 - Applicant interviews only to pump potential employer for information, or vice versa
 - Spy pretends to be a student, journalist, or venture capitalist



Who's Doing It?

- ◆ Foreign governments and corporations
 - Russia, China, South Korea, India, Pakistan, Germany, Israel, Argentina, Taiwan, Indonesia, France, etc.
 - FBI indicates that 57 of 173 nations are running operations to actively target U.S. corporations
 - U.S. “officially” does not participate...(COUGH)
- ◆ Employees
- ◆ Professional industrial spies
- ◆ Members of the Society for Competitive Intelligence Professionals
- ◆ Business consultants (*some in this room?*)
- ◆ H4x0rs (*also some in this room?*)



What's Useful to an Attacker?

- ◆ **Structure** – organization hierarchical structures, departmental diagrams, etc.
- ◆ **Infrastructure** – phone system network diagrams, enterprise IT network diagrams, IT groups, support groups, utilities providers (phone/power/water etc),
- ◆ **People** – Phone directories, e-mail address books, who's who directories etc, visitor instructions, new starter induction packs (i.e., everything you need to know to get around!).
- ◆ **Geography** – super-imposed on hierarchical structures – where is the IT department, where are the servers, etc.
- ◆ **Security Enforcing Functions** – physical access control, password policy, hardware re-use, firewall / IDS use, e-mail policies, phone-use policies, etc.
- ◆ **Networks** – detailed network topologies IP & phone – including firewall, router, and proxy positions.
- ◆ **Software/hardware** – what machines are used, operating systems (service pack & hot fix /patch levels), server software, host software, database software, web server server software, and administration policies.



The Basic Methodology

- ◆ Initial Public Intelligence
- ◆ Social Engineering
- ◆ Physical Security Analysis
- ◆ Network Analysis
- ◆ Information System Attacks



Initial Public Intelligence

- ◆ Meta-Search engines (DogPile, WebFerret), used initially and as more collaborative data is gathered
- ◆ Company searches - the SEC Edgar database (www.sec.gov/edgarhp.htm) - all information is free
- ◆ Gathering names (for later identity spoofing, social engineering, tracing)
- ◆ Gathering phone numbers (for later contacts or war-dialing)
- ◆ Finding IT suppliers (to help determine network components)
- ◆ Check newsgroups, web boards, and industry feedback sites for company info (may yield LOTS of information)



Social Engineering

- ◆ Generally done remotely - requires a degree of deception, masquerade, and motivation
- ◆ Examples are:
 - Gain access privileges by querying administrative personnel over communications medium such as telephone, fax, e-mail, postal mail chat, or bulletin boards from a fraudulent “privileged” position (manager, auditor, law enforcement, etc.)
 - Gain access privileges by querying administrative or help desk personnel over the same mediums as above from a fraudulent “non-privileged” position (confused end user, new contractor, etc.)
 - Invite inside personnel out to a “social business function”, to probe them to disclose information outside of the office (over drinks, strippers, ecstasy, etc.)



Physical Security Analysis

- ◆ Identify monitored access points, coverage, and routes (both by physical guard and/or electronic means)
- ◆ Identify alarm equipment, triggers, response personnel and procedures
- ◆ Identify access privileges through physical access points (side/back doors, under/over fences, windows, roof, weak locks, etc.)
- ◆ Identify weaknesses in the location (line-of-sight visible/audible areas into the target)
- ◆ Identify supply delivery personnel/organizations
- ◆ Identify trash disposal or recycling methods



Network Analysis

◆ Network Survey

- Derive domain name (company name, web presence, etc.)
- Query ARIN for IP blocks and sub-domains
- “dig” domain for DNS servers
- Zone transfer all available DNS domains and sub-domains
- Check public web server source for server links
- Send e-mail and check headers of bounced mails or read receipts
- Search P2P services for organization connections



Network Analysis (cont.)

◆ Network Survey

- War-dial to locate modem-enabled systems and fax machines
- Test for default authentication, easily guessed password, and remote maintenance accounts
- Test for exploitable PBX access
- Attempt PIN-hacking of voice-mail boxes



Network Analysis (cont.)

◆ IP/Port Scanning

- Use broadcast ICMP echo to determine existence of systems
- Try DNS connect attempts on all hosts
- Use “firewalking” to verify ports open through any firewall
- Use nbtstat and “net use” (null session) scans for Netbios (Windows) hosts (port 137)
- Send packets with TCP source port 80 and ACK set on ports 3100-3150, 10001-10050, 33500-33550, 35000-35050 on all hosts
- Send TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 23, 25, 80, and 443 on all hosts



Network Analysis (cont.)

◆ IP/Port Scanning (cont.)

- Send TCP SYN packets on ports 21, 22, 23, 25, 80, and 443 on all hosts
- Send TCP fragments in reverse order to any list of popular ports that may be subject to a variety of exploits
- Use UDP scans on any list of popular ports that may be subject to a variety of exploits
- Use banner-grabbing and other fingerprinting techniques to identify O/S's & apps
- Infer services/protocols/apps via open ports found



Network Analysis (cont.)

- ◆ Retrieve useful information from hidden field variables of HTML forms and from HTML comments
- ◆ Retrieve useful information from application banners, usage instructions, help messages, error messages
- ◆ Retrieve useful information stored in cookies
- ◆ Retrieve useful information from cache or serialized objects
- ◆ Determine wireless access points (wireless sniffer, aéropeek, etc.)



Information System Attacks

- ◆ Use publicly known exploits against identified apps via fingerprinting and port-scanning
- ◆ Attack via default system backdoors (O/S, DB, apps)
- ◆ Use dictionary or brute-force password attacks
- ◆ Gather PDF's, Word docs, spreadsheets and run password crackers on encrypted or protected docs
- ◆ Capture and replay authentication credentials
- ◆ Attack printers to re-route printouts



Information System Attacks (cont.)

- ◆ Use directory traversal or direct instruction attacks on web apps
- ◆ Use long character-strings to find buffer overflows
- ◆ Use cross-side scripting attacks against web apps
- ◆ Execute remote commands via server-side includes
- ◆ Manipulate session cookies, hidden fields, or referrer/host fields to attack server apps
- ◆ Exploit trusted system relationships



Can Organizations Stop It?

- ◆ Identify sensitive information, identify the threats, and provide adequate safeguards (data labeling, access control, encryption, shredding, network access controls, IDS, etc.)
- ◆ Don't ignore security warnings, best practices, or expert advice
- ◆ Educate employees about protecting confidential information
- ◆ Fight for an adequate security budget
- ◆ Have employees, vendors, and partners sign non-disclosure agreements
- ◆ Routinely test all security areas (physical, logical, social, etc.)
- ◆ Sweep for surveillance equipment



Information Warfare



Information Warfare

- ◆ “Information Warfare” – state-sponsored information and electronically delivered actions taken to achieve information superiority in support of national military strategy
- ◆ Meant to affect enemy information and information systems while protecting our information and information systems
- ◆ Includes electronic warfare, surveillance systems, precision strike, and advanced battlefield management



Who's Doing It?

- ◆ Governments
 - China, South Korea, Russia, India, Pakistan, Germany, Israel, Argentina, Taiwan, Indonesia, France, U.S., Al Qaeda, etc.
- ◆ Planted employees
- ◆ Ex-Cold War spies
- ◆ Former intelligence employees
- ◆ Professional hackers
- ◆ PhD's in Computer Science - with millions in government backing
- ◆ The U.S. Air Force, Army, and Navy have established Information Warfare (IW) centers
- ◆ Military information “war games” are now being conducted to prepare for such contingencies (both offensively and defensively)



Information Warfare Categories

- ◆ Offensive - Deny, corrupt, destroy, or exploit an adversary's information, and influence the adversary's perception
- ◆ Exploitative - Exploit available information to enhance the nation's decision/action cycle, and disrupt the adversary's cycle
- ◆ Defensive - Safeguard the nation and allies from similar actions, also known as IW hardening.



Cyber Warfare

- ◆ In the U.S., more than 95% of military communications are conducted over commercial systems (phone, fax, Internet, NIPRNET, SIPRNET, satellite)
- ◆ An increasing amount of technology is being used to fight wars (from un-manned attack systems to cyber-enabled war-fighters)
- ◆ Military information systems and applications drive JTF warfare decisions (personnel/technical assets, logistics, and strategy)
- ◆ The identifiable U.S. targets and their risks have changed drastically



Menu-Driven Warfare

1. Select a nation
2. Identify objectives
3. Identify technology targets
4. Identify communications systems
5. Identify offensive weapons
6. Attack

> Enter your selection:



Cyber Warfare Techniques

- ◆ Initiate virus attacks on enemy systems
- ◆ Intercept telecommunications transmissions
- ◆ Implant code to dump enemy databases
- ◆ Attach worms to enemy radar signal to destroy the network
- ◆ Intercept television/radio signals and modify their content (public psychological warfare)
- ◆ Misdirect radar and content



Cyber Warfare Techniques (cont.)

- ◆ Aggregate pieces of information from many different sources to gain “intelligence” on enemy military capabilities
- ◆ Provide disinformation, such as troop strength, location or number of technical assets
- ◆ DoS enemy computers and communications networks
- ◆ Actively penetrate enemy governmental intelligence and information nodes to steal or manipulate information
- ◆ Modify maintenance systems information
- ◆ Modify enemy logistics systems



Techno-Terrorist Warfare

- ◆ Terrorism (FBI definition) - The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives
- ◆ International Terrorism (CIA definition) – Terrorist activities conducted with the support of foreign governments or organizations and/or directed against foreign nations, institutions, or governments
- ◆ Terrorism (DoD definition) - Premeditated, politically motivated violence perpetrated against a non-combatant target by sub-national groups or clandestine state agents, usually intended to influence an audience
- ◆ Governments and terrorists are **CURRENTLY ACTIVELY PLANNING ATTACKS** on U.S. critical infrastructure components (both in support of military actions, and to turn the general “quality of life” for U.S. citizens to shit)



Techno-Terrorist Warfare Techniques

- ◆ Using a computer, penetrate a control tower computer system and send false signals to aircraft, causing them to crash in mid-air or fall to the ground
- ◆ Use fraudulent credit cards to finance their operations
- ◆ Penetrate a financial computer system and divert millions of dollars to finance their activities
- ◆ Use cloned cellular phones and computers over the Internet to communicate, using encryption to protect their transmissions
- ◆ Use virus and worm programs to shut down vital government computer systems
- ◆ Change hospital records, causing patients to die because of an overdose of medicine or the wrong medicine, or modifying computerized test analysis to alter all future results



Techno-Terrorist Warfare Techniques (cont.)

- ◆ Destroy critical government computer systems
- ◆ Penetrate computerized train routing systems, causing passenger trains to collide
- ◆ Take over telecommunications links or shut them down
- ◆ Take over satellite links to broadcast their messages over televisions and radios
- ◆ And **MOST LIKELY** of all, disrupt power, gas, water, transportation, and telecommunications systems (critical infrastructure components)



Private Investigation



Private Investigation

- ◆ “Private Investigation” – research to develop knowledge on a human subject, by obtaining identifiable private information that can be linked to the individual
- ◆ Used to locate missing people, spy on spouses/friends/acquaintances/enemies, locate birth parents, evaluate prospective employees or business partners, etc.



Personal Identifiers

- ◆ full legal name
- ◆ former names
- ◆ aliases
- ◆ mother's maiden name
- ◆ date of birth
- ◆ social security number
- ◆ drivers license number
- ◆ alien number
- ◆ FBI number
- ◆ current address
- ◆ former addresses
- ◆ hair color/eye color
- ◆ height/weight
- ◆ tattoos
- ◆ physical abnormalities
- ◆ fingerprints
- ◆ photographs/mug shots
- ◆ DNA



Investigation Methods

- ◆ Begin by writing down everything you know about your subject (don't discount any piece of information, no matter how trivial it may appear)
- ◆ Start the investigation from the person's address (if you have it), and work out from there
- ◆ Check city and criss-cross directories at the library
- ◆ Research property records
- ◆ Ask at the Post Office for any change of address on the person
- ◆ Ask neighbors for information
- ◆ Research marriage records



Investigation Methods (cont.)

- ◆ Interview any of the following for detailed info:

Spouse - Former spouses - Mother/Father - Sisters/Brothers - Aunts/Uncles – Children – Grandparents - In-laws – Friends – Landlords - Car dealer – Mechanic – Accountant – Attorneys – Stockbroker – Hairdresser - Insurance agent - Religious affiliations - Gardener/lawn care – Veterinarian – Fellow hobbyists - Financial institutions - Real estate brokers - Medical providers - Child or parental care - Fitness club - Travel agent – Teachers – Children - Maids



Investigation Methods (cont.)

◆ Ask questions such as:

Do you know subject?

How long have you known the subject?

How well did you know the subject?

What kind of work does subject do?

Where did subject work?

Married?

Spouses name?

Any children?

Did subject hang out with anyone in the neighborhood?

Do you know where subject was born and came from?

Do you know where subject's family lives?

Do you know what kind of car subject drives?

Do you know where subject went to school?

Any children away at school?

***continued....



Investigation Methods (cont.)

◆ Continued questions....

Do you know if subject belonged to any organizations?

Did subject ever talk about serving in the military?

Do you know if subject had any help around the house?

Do you know where subject got married?

Divorced? Where? When?

Is subject religious?

Attends what church?

Any interests or hobbies you know of?

Does subject have special medical problems or needs?

Does subject own other property, boats, motor homes, airplanes?

Any problems with drugs or alcohol?

Problems with marital relationship?

Problems with finances?

Do you know where subject is?



Investigation Methods (cont.)

- ◆ Utilize public records resources (discussed in the next several slides)
- ◆ Establish surveillance
 - Tailing
 - Monitoring
 - Electronic techniques

***Because much of this can get into ILLEGAL areas, it makes sense NOT TO DISCUSS specific tools and techniques BEFORE discussing relevant laws (included later in this talk)



Free Public Record Resources

- ◆ Federal Web Locator
<http://www.greenepa.net/~dalex/fedwebloc.html>
- ◆ National Archives and Records Administration
<http://ardor.nara.gov/>
- ◆ National Archives & Records
<http://www.archives.ca/www/svcs/english/PersonnelRecords.html>
- ◆ National Records Center
<http://www.nara.gov/regional/nrmenu.html>
- ◆ US Census Home Page
<http://www.census.gov/>
- ◆ Finding Treasures in the U.S. Federal Census
<http://www.firstct.com/fv/uscensus.html>
- ◆ National Personnel Records Center
<http://www.nara.gov/regional/stlouis.html>
- ◆ Social Security Administration
<http://www.ssa.gov/>
- ◆ IRS
<http://www.irs.ustreas.gov/>



Free Public Record Resources (cont.)

- ◆ Federal Office of Child Support Enforcement
<http://www.acf.dhhs.gov/programs/cse/index.html>
- ◆ National Center for Missing and Exploited Children
<http://www.ncmec.org/>
- ◆ INS
<http://www.ins.usdoj.gov/>
- ◆ Dept. of State Passport Service
http://travel.state.gov/passport_services.html
- ◆ Selective Service Commission
<http://www.sss.gov/>
- ◆ Federal Courts
<http://www.uscourts.gov/>
- ◆ Federal Prison System
<http://www.bop.gov/>
- ◆ Family History Center
<http://www.genhomepage.com/FHC/fhc.html>
- ◆ Social Security Death Index
<http://www.ancestry.com/ssdi/advanced.htm>



National Public Info Database Services

- ◆ AutoTrackXP
 - 1-800-279-7710
 - www.atxp.com
- ◆ ChoicePoint
 - 1-888-333-3356
 - www.choicepointonline.com
- ◆ Lexis-Nexis
 - 1-800-227-9597
 - www.lexis-nexis.com
- ◆ Merlin Information Services
 - 1-800-367-6646
 - www.merlindata.com (best bet and budget, especially for CA)



Types of Public Info Available

- ◆ The four (4) services listed on the previous page can pull the following national, state, and sometimes municipality public records:

Wingate National PeopleFinder – U.S. District Civil & Criminal Court Filings - Bankruptcies – Tax Liens – Boat Registrations – Real Property Ownership – Motor Vehicle Records – Professional Licenses – State Civil Case Filings – State Criminal Case Filings – Voter Registrations – Marriage Records Index – SSN Death Records – Municipal Civil & Criminal Cases (selected) – Divorce Records – Incarceration Records – Accident Records – Boating Citations – Concealed Weapons Permits – Convictions – Handicap Parking Permits - Judgments – Business Credit Reports – Credit Headers – DEA Registrants – Executive Affiliations – FAA Pilots – FAA Aircraft Ownership by Name – FCC Licenses – Federal Employer ID Numbers – Physician Reports by Medi-Net – Significant Shareholders – Address Inspector – UCC Searches – Firearms and Explosives Licenses – Phone Listings – U.S. Military Personnel – TraceWizard Residential Locator – TraceWizard Business Locator – Probable Carrier – National FBNs & Business Filings – Chiropractor Reports – Sexual Offender Registrations – Workers Compensation Records – etc.



Credit Checks

- ◆ There are four (4) national credit reporting services
 - Equifax
 - Experian
 - TransUnion
 - TRW

- ◆ Typical costs for information are:
 - Annual subscription to one service for ~\$70
 - One-time credit check from one service for ~\$10
 - Consolidated one-time report for ~\$30



Lots More Online Resources

- ◆ LOTS of links to free people searches (phone books, e-mail, address, etc.), category searches (adoptees, missing persons, genealogy, etc.), as well as to fee-based people search and private investigation services can be found at:

<http://www.pimall.com>

- ◆ And a few specific popular free search links:

<http://www.switchboard.com/>

<http://www.anywho.com/>

<http://www.dir.org/>

<http://www.555-1212.com/>

<http://www.infoseek.com/>

<http://www.payphones.com/ipp.htm>

<http://netaddress.usa.net/>

<http://worldemail.com/wede4.shtml>

<http://www.yahoo.com/search/people/suppress.html>

<http://www.metacrawler.com/>



Dept. of Justice Databases

- ◆ Alien Status Verification Index System (INS)
- ◆ Automated Biometric Identification System (INS fingerprint database)
- ◆ Automated Intelligence Records System (DEA, INS, Coast Guard)
- ◆ Central Index System (INS)
- ◆ Confidential Source System (DEA)
- ◆ Controlled Substances Act System (DEA)
- ◆ DEA Aviation Unit Reporting System (DEA)
- ◆ Deportable Alien Control System (INS)
- ◆ Domestic Security/Terrorism Investigations Records System (Office of Intelligence)
- ◆ Drug Testing Program Record System (DEA)
- ◆ Electronic Surveillance Tracking System (Criminal Division)
- ◆ Essential Chemical Reporting System (DEA)
- ◆ Fingerprint Identification Records System (FBI)
- ◆ Grants of Confidentiality Files (DEA)
- ◆ Inappropriate Communications/Threat Information System (U.S. Marshals)



Dept. of Justice Databases (cont.)

- ◆ Information Support System (Natl. Drug Intelligence Center)
- ◆ International Intelligence Database (DEA)
- ◆ Narcotics and Dangerous Drugs Information System (DEA)
- ◆ National Automated Immigration Lookout System II (INS)
- ◆ National Crime Information Center (FBI) **
- ◆ National DNA Index System (FBI)
- ◆ National Drug Pointer Index (DEA)
- ◆ National Instant Criminal Background Check System (FBI) **
- ◆ Security Clearance Forms for Grand Jury Reports (U.S. Attorneys Executive Office)
- ◆ Sentry (Federal Bureau of Prisons)
- ◆ Threat Analysis Information System (U.S. Marshals)
- ◆ Warrant Information System (U.S. Marshals)
- ◆ Witness Immunity Tracking System (Criminal Division)



Are You Under Surveillance?

- ◆ Your garbage disappears before the trash collection passes
- ◆ Suspicious people or vehicles appear in multiple locations
- ◆ Others know your activities when they shouldn't
- ◆ Confidential business information seems to be known to others
- ◆ Someone tells you that someone else was asking questions about you
- ◆ You have been the victim of a burglary, but nothing was taken
- ◆ Electrical wall plates appear to have been moved slightly
- ◆ You've noticed static, popping, scratching, strange sounds, beeps, or volume changes on your phone lines
- ◆ Sounds are coming from your phone's handset when it's hung up (check by using an external amplifier)
- ◆ Your phone rings and nobody is there, or a very faint tone or high-pitched beep is heard



Are You Under Surveillance? (cont.)

- ◆ Your radio or television has suddenly developed strange interference
- ◆ Your car radio makes strange sounds
- ◆ Dime-sized discolorations appear on the wall or ceiling
- ◆ Someone just gave you any type of electronic device (desk radio, alarm clock, lamp, small TV, boom box, CD player, etc.)
- ◆ A small bump has appeared on the vinyl baseboard near the floor
- ◆ The smoke detector, clock, or lamp in your office/home looks slightly crooked, has a small hole in the surface, or has a quasi-reflective surface
- ◆ Certain items have appeared in your office or home, but no one knows where they came from
- ◆ Drywall dust or debris is noticed on the floor next to the wall



Are You Under Surveillance? (cont.)

- ◆ You notice small pieces of ceiling tiles or grit on the floor or on the surface of your desk
- ◆ You notice that “phone company” trucks and utilities workers are spending a lot of time near your home or office doing repair work
- ◆ Telephone, cable, plumbing, or air conditioning repair people show up to check something out when no one called them
- ◆ Service or delivery trucks are often parked nearby with nobody in them
- ◆ Your door locks suddenly don’t feel right (sticky or failing)
- ◆ Furniture has been moved slightly
- ◆ Things seem to have been rummaged through



Tools of the Trade

Truth Phone

- ◆ Lie Detection
- ◆ Desktop phone
- ◆ Conversation Recorder



Wireless Video Sunglasses

- ◆ Discretely videotape from hidden camera
- ◆ Real-time Video



Video Pen

- ◆ Recording live events
- ◆ Compact size



Tie Camera

- ◆ Housed in “stylish” Italian ties
- ◆ Compact



Night Vision Monocular

- ◆ Cold war technology
- ◆ High image quality & range
- ◆ No Batteries
- ◆ Price: \$274.95



Laser Listening Device

- ◆ No Transmitter
- ◆ Clear night laser technology
- ◆ High range
- ◆ Price: \$ 349.95



Portable Voice Changer

- ◆ Easy to connect to your phone
- ◆ Up to 8 profiles
- ◆ Built in amplifiers
- ◆ Price: \$ 99.95





BloodHound

- ◆ Bug/wire detector
- ◆ Advanced RF detector
- ◆ Microphone detector
- ◆ Price: \$ 249.95





Identification Credentials

- ◆ Fake ID's (drivers licenses, work badges, etc.)
- ◆ Diplomas
- ◆ Law Enforcement Badges
- ◆ Government Employee ID
- ◆ Passports
- ◆ Professional Licenses
- ◆ Press Credentials



Important Laws



Wiretaps

- ◆ 18 USC 2510 - *Electronic Communications Privacy Act of 1986* – Unauthorized interception of an electronic communication (whether recorded or not)
- ◆ Includes phone, pager, cell phone, cordless phone, fax, or data transmission (got sniffer?)
- ◆ Penalties include up to 5 years imprisonment, criminal fines, possible civil liability
- ◆ Law also prohibits illegally intercepted communications from being entered as evidence in court
- ◆ Law ALSO makes it illegal to use an electronic device to listen to or record oral communications, under same penalties



Recording Phone Calls

- ◆ Wiretap law applies (previous slide)
- ◆ Some notable exceptions:
 - Calls can be recorded with consent of at least ONE party (***) 12 states require consent by BOTH parties – CA, CT, DE, FL, IL, MD, MA, MI, NE, NH, PA, WA)
 - Businesses may monitor business-related phone calls of employees, using phone company equipment only
 - 48 CFR Sec.64.501 (FCC) requires that at least ONE of the following occur:
 - Both parties consent
 - Recording party gives verbal notification before recording
 - Must be a regular electronic beep tone during recording



Surveillance

- ◆ Established by “case law”, not “statute”
- ◆ Non-threatening observation and/or photography from publicly accessible areas is acceptable, whereas trespassing on private property or altering environment (cutting holes in bushes/fences) to aid viewing is not
- ◆ Penalties include civil liability for “invasion of privacy” or “harassment”, if surveillance is obtrusive or threatening



Freedom of Information Act

- ◆ 5 USC 552 - *Freedom of Information Act (FOIA)* - Allows public access to certain federal government records
- ◆ Doesn't apply to state, local government, Congress, or White House courts (however, all states have their own FOIA versions as well)
- ◆ “Exclusions” are: current law enforcement investigations, C.I. disclosure, FBI records related to terrorism or espionage
- ◆ There are also many “exemptions”, which MAY be released unless prohibited by other laws or if their release would cause no foreseeable harm
- ◆ No penalties for violation (at least directly)
- ◆ Call 1-800-688-9889 to obtain FOIA “officer contact info” for any federal agency



Privacy Act

- ◆ 5 USC 552a - *Privacy Act of 1974* – Allows any citizen to view and amend (if incorrect) any federally maintained database information about himself/herself
- ◆ Also sets forth guidelines for federal agencies to follow when collecting and using data (i.e., name, SSN)
- ◆ Penalties for persons obtaining information under false pretense OR for federal employees improperly releasing information include misdemeanor conviction and up to \$5K fine
- ◆ Civil remedies can be obtained against government agencies that violate the act



Mail Inspection

- ◆ 18 USC 1702, 1708 - *Obstruction of Correspondence & Theft or Receipt of Stolen Mail* – It is a crime to take, steal, or remove any mail without permission
- ◆ Penalties include fines, imprisonment up to 5 years, possible civil liability for invasion of privacy



Trash Inspection (Dumpster Diving)

- ◆ Established by “case law”, not “statute”
- ◆ US Supreme Court ruled that “any person who places his/her trash at the curb of a public street for pickup has no reasonable expectation of privacy over the trash”
- ◆ If trash is located in area marked as “private” or “no trespassing”, “diving” is obviously illegal
- ◆ Exceptions:
 - Several municipalities have local ordinances making curbside trash off limits to anyone but the “trash man”
 - Hawaii, New Jersey, Washington, and Vermont may have state supreme court rulings which conflict with US Supreme Court ruling
 - At least one exception allows trash to be turned over to police after being picked up
- ◆ Penalties include civil and criminal penalties for trespassing and invasion of privacy where collection is made from private property
- ◆ Local municipalities may have additional limited penalties



Economic Espionage

- ◆ 18 USC 1831 - *Economic Espionage Act of 1996* – Obtaining a trade secret from a U.S. business without authorization and providing it to a foreign government, agent, or company is a federal crime
- ◆ Penalties include up to 15 years imprisonment, fines up to \$10,000,000, and civil liability



Computer Crime (H4x0ring)

- ◆ 18 USC 1030 - *Fraud and Related Activity in Connection with Computers* – Unauthorized access into the computer of a government, business, or person is a federal crime if the entry includes removal/copy of information, destruction of files, or the planting of any code or virus
- ◆ Penalties include up to 10 years imprisonment, fines, and persons harmed by unauthorized access can sue for compensatory damages and injunctive relief
- ◆ When unauthorized access to a computer occurs and the only fraud is use of the computer and the value of such use is less than \$5K in any one year, **NO CRIME HAS BEEN COMMITTED**
- ◆ Also crimes under this statute:
 - Trafficking in computer passwords with the intent to defraud is also a crime under this statute
 - Any threat sent via computer with intent to extort money or anything of value
- ◆ Several states have implemented more restrictive (simple trespass) laws



Stored Communications

- ◆ 18 USC 2701 - *Electronic Privacy Communications Act of 1986* – Unauthorized access to electronically stored communications (such as e-mail or telegrams) is a federal crime
- ◆ Penalties include up to 2 years imprisonment, civil action by aggrieved party to recover actual and punitive damages
- ◆ Civil actions must be filed within 2 years of the violation discovery date



Other Laws of Interest

- ◆ 18 USC 701, 712, 912, 913 – *Impersonation of a Federal Official*
- ◆ 18 USC 1905 – *Disclosure of Confidential Information*
- ◆ 26 USC 6103 – *Confidentiality and Disclosure of Returns and Return Information*
- ◆ 18 USC 3534a - *Government Information Security Reform Act of 2000*
- ◆ Public Law 104-191 - *Health Insurance Portability and Accountability Act of 1996*
- ◆ 18 USC 2721 – *Driver Privacy Protection Act*
- ◆ 29 USC 2001 - *Employee Polygraph Protection Act of 1988*
- ◆ 18 USC 2710 – *Wrongful Disclosure of Videotape Rental or Sales Records*
- ◆ 15 USC 1692 – *Fair Debt Collection Practices Act*
- ◆ Public Law 106-102 – *Financial Services Modernization Act of 1999*
- ◆ 15 USC 1681 – *Fair Credit Reporting Act*
- ◆ 39CFR265.6 – *Code of Federal Regulations*
- ◆ 20 USC 1232g – *Family Educational Rights and Privacy Act*



Law Wrap-up (finally)

- ◆ Full text of most laws referenced in this presentation can be found at: <http://www4.law.cornell.edu/uscode/>

Presentation Wrap-up

- ◆ What have we learned?

Intelligence Gathering

QUESTIONS??

