CS 526: Information Security

Legal Issues
Unusual times

• Cyber law relatively new
  – Not enough time & cases

• Liability “grace period”
  – Legal system confusion
  – Insurance industry confusion
    • How to assess and price risk

• Historical precedents from other technologies
  – Eventually, there is clarity (but it can take a while)
Who has jurisdiction?

• Usually, local or state authorities
• Must contact Federal authorities if
  – Classified or military or nuclear information
  – Equipment used by federal agency
  – Bank or regulated financial information
  – Interstate telecom
  – Offenders are from out of state
Whose community standards apply?

• Live in X but web page readable from Y
  – Can be sued in Y
  – Y’s community standards
    • Possibly very different from X’s

• U.S. v.s. some couple
  – X = Milpitas, CA
  – Y = Memphis, TN
U.S. Federal Laws

• Fraudulent use of credit cards
• Copyrights
  – Infringements, remedies
• Embezzlement and theft
• Espionage
• Censorship
• Fraud and false statements
• Mail fraud and swindles
Laws (cont’d)

- Records and reports
  - Concealment, removal, mutilation
- Sabotage
- Stolen property
- Communications interception
- Privacy protection
- Malicious mischief
Laws (cont’d)

• Theft
• Unauthorized use
• Trespass
• Tampering (various degrees)
• Unlawful duplication
• Criminal possession
• Theft of services
Laws (cont’d)

• Forgery
• Eavesdropping
• ...

International laws

• Country-dependent
• Significant differences between countries
  – Restrictions on cryptography
    • Domestic restrictions
    • Import / export restrictions
  – Burden of proof
  – Privacy
  – Language laws
    • U.S. university sued in France (English-only web site)
Privacy

• Fundamental human right
  – In most constitutions
• First law in 1361 against peeping toms and eavesdroppers
• In 1948’s Universal Declaration of Human Rights
The reality ...

• Surveillance authority abuse
  – Widespread violations
    • Degree varies by country
    • Perpetrators are usually police, companies, criminals, ...

• Targets
  – Opposition politicians
  – Journalists
  – Human rights activists
The reality ...

• Erosion from new technologies
  – ID systems (ID cards, biometrics, …)
  – Communication surveillance
  – Video surveillance
  – Workplace surveillance
Privacy and data protection laws

• Many purposes
  • Prevent government abuse
  • Promote e-commerce
  • Achieve compatibility with other countries
Privacy and data protection laws

• Vary among countries (mainly by degrees)
• Require personal information to be:
  – Obtained lawfully
  – Obtained fairly
  – Used only for the original specified purpose
  – Adequate, relevant and not excessive to purpose
  – Accurate and up to date
  – Destroyed after its purpose is completed
Privacy Protection: Self-regulation

• Codes of practice
  – Industry-specific
  – E.g., “American XYZ Association” would issue privacy guidelines and codes for the XYZ industry

• Proved disappointing
  – Resulted in inadequate codes
  – Codes of practice were not enforced
  – Inherently conflicted to have regulator = regulated
  – Failure was predictable (why was it even tried?)
Regulatory Privacy Protection

• Comprehensive data protection law
• Enforcement through a public official
  – Monitors compliance
  – Investigates breaches
• No delay when new technologies appear
  – Existing law applies to all current and future products and technologies
• EU, CA, Australia, NZ, HK, ...
Sectoral Privacy Protection

• Sectoral laws: One for each sector and technology
  – Movie rental/viewing) records
  – Financial records (Gramm-Leach-Bliley)
  – Medical records (HIPAA)
  – Students records (FERPA)
  – ...
  – Enforcement through many mechanisms

• Used in U.S.

• Laws lag behind technology
  – E.g., genetic information
Hybrid (Regulatory + Sectoral)

• A comprehensive law, complemented with sectoral laws
• Sectoral laws provide more detailed protection of certain categories of information, such as
  – Police files
  – Consumer credit records
  – ...

DIY Privacy Protection

• Individual self-protection
• Using privacy and anonymity technologies
  – Anonymous browsing (e.g., using Tor)
  – Paying with digital currencies (e.g., digital cash or a crypto-currency like Bitcoin)
  – In the extreme, can disappear (no bank account, no permanent address, burner phones, ... )
• Cannot replace a legal framework
Search Warrants

• Requires probable cause before judge approves
  – Police required to explain how they plan to limit the search before the warrant may be granted
  – Police can seize items observed in plain view (even if not in the warrant)

• Limited time for examining seized equipment
  – Forensic analysis of seized equipment must be conducted “within reasonable time” (can vary depending on data size, presence of encryption, etc)
  – In a 2009 case, courts deemed 21 days “excessive”
Digital Search Warrants (cont’d)

• Can police keep the seized data indefinitely for use in future criminal investigations?
  – No: Courts have ruled that it would violate the Fourth Amendment of the U.S. Constitution (which protects people’s right to privacy and freedom from arbitrary governmental intrusions)
  – Evidence obtained in violation of the Fourth Amendment cannot be used in court

• Can search without warrants at U.S. borders
Criminal prosecution

• Government pays
• Special difficulties
  – What is admissible evidence
  – Proving a specific person was using the computer when the crime occurred
  – Standards of proof
• Lack of trained personnel
• Corporate reluctance to report e-crimes
  – Widespread underreporting
Civil lawsuits and liability

• Litigants pay
• Intellectual property
• Publicity
  – E.g., photo of Alice on web without her permission
• Negligence
• Spamming
• Spoofing

[ Historically, new technologies => more lawsuits ]
Civil lawsuits and liability

• Defamation
  – Editorial control as a hazard
    • Stratton Oakmont v.s. Prodigy (1995)
  – As of 1996: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another”

• Importance of prior consent
  – Who owns email, files, ...etc?
  – Organization’s e-policy must explicitly state it
    • Word it so purpose is self-protection (not intrusiveness)
    • Evenly investigate and evenly enforce
Negligence

• Failure to disclose security risks
• Failure to use latest technologies
• Failure to operate technologies properly
• Failure to establish appropriate policies
• “Standards of due care”
• One-sided liability
• Negligence impacts legal responsibility
  – E.g., in case of large losses caused by employee or outsider misbehavior (“computer amplified” damage)
Intellectual Property: Trademarks

• A trademark identifies the brand owner of a particular product or service
  – Usually a recognizable sign, design, or expression
  – Can be licensed by its owner to other parties

• Trademark infringement / dilution
  – “Famous” mark (infringers confuse consumers)
  – Hasbro vs. candyland.com
  – Planned Parenthood vs plannedparenthood.com
  – Porsche vs. porsch.com, porsche.net, ...
Intellectual property: Domain Names

• Domain name battles
  – wwwpainewebber.com (note the missing “.”)
    + injunction against NSI
  – clue.com (Mattel vs. Clue Computing Inc.)
  – Etoys vs. www.etoy.com

• Anti-cybersquatting law
  – cybersquatting = acquiring a domain name in bad faith (e.g., with intent to later sell it to a legitimate trademark holder)
  – typo-squatting
Intellectual Property: Copyrights

• Copyright = exclusive right that the creator of an original work has to its use/dissemination
  – Even if no explicit sign

• Protected under digital copyright law

• Direct infringement
  – “Strict liability” rule: It does not matter whether the infringer thought he was breaking the law
Copyright Infringement

• Contributory infringement
  – Knowingly contribute to infringement by other(s)

• Vicarious liability
  – Benefit financially from another party’s infringement, and
  – Having control over that other party’s
Copyrights: Liability Limits

- DMCA contains “safe harbor” provisions that limit the liability of certain organizations
- Some special condition must hold, e.g.,
  - “Mere conduit”
  - Caching
  - Hosting
- Examples
  - An ISP
  - A university
Intellectual Property: Patents

- Patent = Exclusive legal rights to invention
  - Granted to inventor or assignee
  - Granted by a specific country
  - Limited in time (expiration date)
  - Requires public disclosure of the invention
  - Solution to a specific technological problem (can be a product or a process) defined by claims
  - Solution must be novel, useful, and non-obvious
  - Can be difficult to enforce (even to detect)
Intellectual Property: Patents (cont’d)

• Defensive publication
  – Detailed public disclosure of invention for the purpose of preventing others from patenting it
  – Establishes “prior art”
  – Can be anonymous

• An alternative to patent: Trade secret
  – Invention is kept confidential (no time limit)
  – Use nondisclosure and employment agreements
  – Can be vulnerable to reverse engineering
Reverse-Engineering

• OK if for certain purposes (e.g., interoperability)
• Lexmark v.s. Static Control
  – Static Control had reverse-engineered Lexmark chips for the purpose of making and selling cartridges that are compatible with Lexmark printers
  – Court upheld the right of Static Control to make parts that interoperate with goods of another manufacturer
  – Static Control could afford the legal fight, an individual researcher (professor or grad student) typically cannot
• Anti-competitive practices are rife (not only in printers)
  – Cell phone batteries, automobile parts, ...
Reverse-Engineering (cont’d)

• HP OfficeJet episode
  – On 9/13/2016, a firmware update from HP deliberately caused all HP OfficeJet printers to reject non-HP ink cartridges
  – On 9/12/2016 a customer had a working printer, one day later it no longer worked
  – The non-HP ink cartridge makers will (try to) produce cartridges that work with the new firmware

• Some auto manufacturers now claim to own parts of a vehicle you bought and fully paid for
DMCA and Reverse Engineering

• Section 1201 of DMCA forbids “circumvention of copyright protection systems”
  – Provides both criminal and civil penalties
  – Not just for music and movies: Applies to software and hardware (even multi-purpose, as long as a purpose pertains to copyright protection)

• Has been used to prevent reverse engineering
  – Even when done by responsible researchers whose purpose is to analyze the security of deployed systems, inform their manufacturers of the flaws discovered, and help them fix those flaws
DMCA & Reverse Engineering (cont’d)

• When honest, responsible researcher informs manufacturer of discovered flaws, the typical reaction is a threat of a lawsuit under DMCA
  – Manufacturer’s do not want their products’ internals investigated, use DMCA to prevent it

• Manufacturers’ motivations include:
  – Embarrassment caused by disclosure of the flaws
  – The costs they’d have to incur to fix the flaws
  – The “flaws” might be deliberate (and illegal)
DMCA Lawsuits

• Such lawsuits work against honest researchers
  – They cannot afford the legal costs of fighting them
• But criminals don’t care about DMCA lawsuits
  – They quietly exploit the flaws they discover (and they too don’t want anyone else finding the flaws)
  – Many criminals, highly motivated: They find flaws
• Result: Many flaws in systems remain unfixed
  – Known to criminals, but not to the public
DMCA’s (Un)intended Consequences

• DMCA prevented access to the VW emissions-cheating software
  – The software caused vehicles to “pass” emissions tests even though they’d fail in normal use conditions
  – Access to the software would have revealed the code fragments responsible for the cheating

• Researchers routinely refrain from disclosing serious vulnerabilities they find
  – For fear of being jailed under DMCA
  – Foreigners who do disclose, avoid travel to the U.S.
DMCA and the U.S. Constitution

• It is in the public interest to allow honest researchers to find, responsibly disclosure, discuss, and help fix flaws in deployed systems
  – To prevents this threatens U.S. national security

• Such discussions are legitimate free speech
  – Protected by the U.S. Constitution

• First Amendment to the U.S. Constitution
  – “prohibits the making of any law ... abridging the freedom of speech, infringing on the freedom of the press, ...”
More Examples of DMCA Lawsuits

• Viacom v. *YouTube and Google
  – Filed 2007 sought $1B in damages
  – 2010: Judgement in favor of YouTube (“mere conduit” defense), Viacom appealed
  – 2012: The 2010 judgement is vacated
  – 2013: The 2010 judgement is reaffirmed

• *Lenz v. Universal Music Corp
  – Lenz had posted home-made video on YouTube whose removal was forced by Universal under DMCA
Admissible evidence & testimony (1)

• Legally obtained evidence
• “Fairly” obtained evidence
• No hearsay
  – Audit Logs are hearsay (inadmissible), unless they are “records of regularly conducted activity”
  – Make logs part of business routine
• Clear chain of custody
  – Put in empty locked room? (not OK if janitor has access)
Admissible evidence & testimony (2)

• Expert-level tech evidence
  – Tested
  – Low error rate
  – Published in peer-reviewed journal (or otherwise widely accepted)

• Accuracy
  – Raw event logs are OK (for accuracy)
  – Info derived from event logs can lead to intense cross-examination
Admissible evidence & testimony (3)

• Transparency
  – No secret mechanism
  – Assume the hackers know it
  – Better than obscurity
After a break-in

• Talk to a lawyer before legal action
• Should you take legal action?
  – Insurance company may insist you do
  – The law may require it
  – Failure to do so may
    • make you liable
    • anger employer
    • anger shareholders
Frontier justice

• Some lawyers’ USENET (mis)adventures
  – Advertised (massively) their immigration advisory services
  – Suffered retaliation (with impunity), e.g.,
  – Fake mail orders, fake pizza orders
  – “Cancelbots”
  – Spamming
  – ...
  – Their ISP terminated their service