Today

- Legal Issues: Liability

Homework

- Exercise Set 6 due
- Exercise Set 7 out (due next week)
- Essay # 3 out
- Quiz next Wed
Legal Issues and Responsibilities ...

Topics we’ll look at:

• Liability/protections (part 1)
• Intellectual property (part 2)

Liabilities and Protections

_**Liability:**_ what “harms” to consumers is a software maker responsible for?

_**Protection:**_ what consumer protections against “harms” are there?

Our focus is on _liability_

• Protection usually refers to legal ability to recoup losses
• Although protection & liabilities aren’t always opposites
  – e.g., banks and FDIC
Legal Liabilities

Involved parties in software damages

- Software “producers” ... company, vendor, developers
- Software “consumers” ... end users, clients, intermediaries
- Third parties, e.g., hackers, thieves, governments

Can be complex: e.g., using Amazon EC2 in your app

Broad areas of damages ...

- Software that breaks laws (e.g., theft, national security, )
- Software that results in personal harm (e.g., GPS case)
- Quality issues that lead to direct/indirect financial/privacy loss

Well focus on financial/privacy loss which is largely:

**Buyer Beware!**

- Software producers have limited liability
- Software consumers shoulder majority of damages

There are a number of reasons for this ...
1. Lack of legislation ("legislative void")
   - Few laws specific to software
   - Some do exist:
     - CAN-SPAM act of 2003
     - State data-breatch notification laws
     - CFAA (computer fraud & abuse act)

2. Disputes often fall under "contract law"
   - as opposed to criminal or tort law
   - Tort law requires more than "purely economic damages"
   - typically physical damage (personal or property)

Software sometimes protected under the **Uniform Commercial Code (UCC)**
   - Not a law, but suggestions to states ... however, adopted by most states
   - Legal rules around contracts and contract disputes including warranties
   - Only applies to "goods" and not "services"
   - If software viewed as a good, UCC applies (e.g., with warranty protections)
Most software today is “licensed” and not purchased

- i.e., users don’t actually own the software (e.g., GM\(^1\))
- “End User License Agreement” (EULA) ... downloaded
- “Terms of Service” (TOS) ... e.g., web sites

Courts usually allow software licenses to disclaim liabilities for product deficiencies

3. **Free software is not considered under contract law ("considerations")**

- No buyer and seller to form a proper contract

---

\(^1\) [www.autoblog.com/2015/05/20/general-motors-says-owns-your-car-software/](www.autoblog.com/2015/05/20/general-motors-says-owns-your-car-software/)
Some examples ...

LinkedIn 2012 class action suit

• brought against it after hackers caused a data breach
• caused 6.5 million password hashes to be released
• 60% of the passwords were later cracked
• part of claim was that it used “weak password security” (no salt)
• passwords obtained through an SQL injection attack

Results:

• Plaintiffs argued LinkedIn failed to utilize industry standard techniques to protect data, in violation of its own User Agreement and Privacy Policy
• A federal court in California threw out most claims on the grounds that the policy was the same for users of the free and premium versions of the service
• The court found that the complaint “fails to sufficiently allege that Plaintiffs actually provided consideration for the security services which they claim were not provided”
• LinkedIn settled with the much smaller number of “paying” LinkedIn customers (800,000 versus 6 million) a total of $1.25 million (which after fees is about $1 per paying user)
In 2011, Facebook was sued for sharing data with third parties

- in violation of their own published policies
- a major issue was that Facebook was providing identifying data to advertisers

Results

- The judge ruled against the claims, in part because Facebook is free to use:

  "[A] plaintiff who is a consumer of certain services (i.e., who paid fees for those services) may state a claim under certain California consumer protection statutes when a company, in violation of its own policies, discloses personal information about its consumers to the public. Here, by contrast, Plaintiffs do not allege that they paid fees for Defendants services."
4. Security is viewed as hard ...

- some courts have treated security expectations as inherently unreasonable (since software cannot be made bug free)

5. Hackers cause the problems ...

- some courts have rejected claims since 3rd party hackers create the issue
- and the vendors don’t benefit from these attacks (e.g., Sony employee data breach case)
End User License Agreements (EULAs)

Shrinkwrap, Clickwrap, Browserwrap agreements

- All represent a (service) contract between a buyer and seller

- However, to be a valid contract, it must ...
  - be conspicuous
  - be an offer (seller) and acceptance (buyer)
  - have considerations
  - involve a "meeting of the minds" ... you know it is legally binding, and a shared understanding of terms
  - plus others (e.g., legal activities)
Examples of EULA’s not passing as contracts

Zappos.com suffered a security breach and was sued

- Asked for arbitration because the TOS on its website required all disputes to be “submitted to confidential arbitration in Las Vegas, Nevada.”

- The EULA was part of a browserwrap agreement that users were not required to affirmatively “accept” … a link was located in the footer of the homepage you had to scroll to see

- The District of Nevada Court concluded that plaintiffs never viewed, let alone manifested assent to, the TOS,

- and held that the arbitration provision was unenforceable

- Similar case with Barnes & Noble (suit against cancelled orders)
Liability “extremes”

The two extremes:

- Buyer beware
- Hold software producers responsible

Where we seem to be today:

- Somewhat murky middle ground
- But (slowly) heading more towards 2?
Some history: Late 1990s UCITA
(Uniform Computer Information Transactions Act)

- To deal with issues with the Uniform Consumer Code
- Proposed making software producers automatically liable for defects/errors
- **Supporters**: large software companies (Microsoft, Adobe, ...)
- **Opposers**: IEEE, ACM, Free Software Foundation, FTC, ...

Q: Why do you think the opposers and supporters took these positions? ...

Why was UCITA opposed?

- Allowed shrinkwrap licenses to override UCITA provisions
- But free software could not override UCITA provisions
  - Weakened consumer protections
  - Allowed licensing over purchases
- Which weakens consumer protections

Only passed in two states, but with amendments

Some states even passed anti-UCITA laws

Exercise Sheet ...
Liability “extremes”

Arguments against Buyer Beware:

1. Software is critical/essential part of peoples lives

2. Most users cant make security decisions (sophistication)

3. Anti-virus software cant keep up ...
   - Already a multi-billion dollar industry
   - about 15% of antivirus software is fake / malware

4. Economics of software is build first, patch later
   - Places burden on users (who must apply patches)
   - e.g., 52% of IE users dont use latest version

5. Without incentives for quality, situation becomes worse
   - Which increases the potential damages
   - High-profile cases increases the cost on software makers
   - Which goes against the buyer beware model
Arguments for software producers taking responsibility:

1. Software doesn’t follow standards applied to other industries
   • E.g., as a renter, if you don’t provide industry standard locks, you can be held liable for damages

2. Many software problems are easy to fix
   • marketplace just doesn’t reward it

3. Not requiring responsibility translates to government subsidy
   • Companies can produce more products faster/cheaper

4. Other countries moving in this directly already …
Opinions can quickly change

The automotive industry as an example

- In the 60’s, courts reluctant to apply tort laws for defects
- Over next 30 years, did an “about face”
- Started in 1966 with the National Traffic and Motor Vehicles Safety Act
- Giving the government the power to create & enforce safety standards

Cost of software “harms” are on the rise!

- e.g., thousands of data breaches every year! (+ undetected)

In 2016, per company²

- Avg total cost of a data breach in US is $7 million
- Avg cost of detecting a breach is $1.6 million
- Avg cost of notification is $590,000 (laws for this)
- Avg cost of lost business is $3.9 million
- Avg cost of handling breach $1.7 million (incl. legal costs)
- 24% chance of a data breach within 24 mo period

²2016, Ponemon Institute LLC and IBM
Proposed US laws already coming!

- Recently a US Senator proposed\(^3\) similar laws to GDPR
- Legislation allows FTC to write and enforce privacy regulations
- Impose large fines and up to 20-year prison sentences for violations