Computers and the Law

Randy Canis

CLASS 11

DMCA pt. 1;
Software Licensing pt. 1;
Data Security
DMCA pt. 1

DMCA

- The DMCA is the Digital Millennium Copyright Act that was signed into law on October 28, 1998.
- The DMCA amended and augmented parts of the existing Copyright Act (i.e., Title 17).

Universal Studios v. Reimerdes

- Universal Studios et al. (P)
  - Eight major motion picture studios.
- Reimerdes (D)
  - Poster of DeCSS software program.
- Basis of Proceeding
  - Decision after preliminary injunction in favor of the P.

Universal Studios v. Reimerdes

- What is CSS?
- How was CSS maintained?
- What is DeCSS?
- What did the D do?
  - Defendants posted the source and object code for DeCSS on the 2600.com web site, from which they could be downloaded easily. ... 2600.com contained also a list of links to other web sites purporting to post DeCSS.

Universal Studios v. Reimerdes

- Why do the movie studios care about DeCSS and its progeny?
- “First, the availability of DeCSS on the Internet effectively has compromised plaintiffs' system of copyright protection for DVDs, requiring them either to tolerate increased piracy or to expend resources to develop and implement a replacement system unless the availability of DeCSS is terminated.”
- “Second, the application of DeCSS to copy and distribute motion pictures on DVD, both on CD-ROMs and via the Internet, threatens to reduce the studios' revenue from the sale and rental of DVDs. It threatens also to impede new, potentially lucrative initiatives for the distribution of motion pictures in digital form, such as video-on-demand via the Internet.”

Universal Studios v. Reimerdes

- The DMCA contains two principal anticircumvention provisions.
- The first, Section 1201(a)(1), governs “[t]he act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work,” an act described by Congress as “the electronic equivalent of breaking into a locked room in order to obtain a copy of a book.”
- The second, Section 1201(a)(2), which is the focus of this case, “supplements the prohibition against the act of circumvention in paragraph (a)(1) with prohibitions on creating and making available certain technologies developed or advertised to defeat technological protections against unauthorized access to a work.”
- As defendants are accused here only of posting and linking to other sites posting DeCSS, and not of using themselves to bypass plaintiffs' access controls, it is principally the second of the anticircumvention provisions that is at issue in this case.
Universal Studios v. Reimerdes
Section 1201(a)(2)(A)

(1) CSS Effectively Controls Access to Copyrighted Works

• "First, the statute expressly provides that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information or a process or a treatment, with the authority of the copyright owner, to gain access to a work.""

Universal Studios v. Reimerdes
Section 1201(a)(2)(B)

• As the only purpose or use of DeCSS is to circumvent CSS, the foregoing is sufficient to establish a prima facie violation of Section 1201(a)(2)(B) as well.

Universal Studios v. Reimerdes
Statutory Exceptions: Reverse engineering

• Defendants claim to fall under Section 1201(f) of the statute, which provides ... in substance that one may circumvent, or develop and employ technological means to circumvent, access control measures in order to achieve interoperability with another computer program provided that doing so does not infringe another's copyright and, in addition, that one may make information acquired through such efforts "available to others, if the person [in question] ... provides such information solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement." ... They contend that DeCSS is necessary to achieve interoperability between computers running the Linux operating system and DVDs and that this exception therefore is satisfied. ... This contention fails.
Universal Studios v. Reimerdes

- Fair use
- Finally, defendants rely on the doctrine of fair use. Stated in its most general terms, the doctrine, now codified in Section 107 of the Copyright Act, ... limits the exclusive rights of a copyright holder by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes, free of liability for copyright infringement. For example, it is permissible for one other than the copyright owner to reprint or quote a suitable part of a copyrighted book or article in certain circumstances. The doctrine traditionally has facilitated literary and artistic criticism, teaching and scholarship, and other socially useful forms of expression. It has been viewed by courts as a safety valve that accommodates the exclusive rights conferred by copyright with the freedom of expression guaranteed by the First Amendment.

Universal Studios v. Reimerdes

- Defendants therefore argue that the DMCA cannot properly be construed to make it difficult or impossible to make any fair use of plaintiffs' copyrighted works and that the statute therefore does not reach their activities, which are simply a means to enable users of DeCSS to make such fair uses. Defendants have focused on a significant point. Access control measures such as CSS do involve some risk of preventing lawful as well as unlawful uses of copyrighted material. Congress, however, clearly faced up to and dealt with this question in enacting the DMCA.

Universal Studios v. Reimerdes

- "The Court begins its statutory analysis, as it must, with the language of the statute. Section 107 of the Copyright Act provides in critical part that certain uses of copyrighted works that otherwise would be wrongful are "not ... infringement[s] of copyright." Defendants, however, are not here sued for copyright infringement. They are sued for offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act. If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate."

Universal Studios v. Reimerdes

- "Defendants claim also that the possibility that DeCSS might be used for the purpose of gaining access to copyrighted works in order to make fair use of those works saves them under Sony Corp. v. Universal City Studios, Inc. But they are mistaken. Sony does not apply to the activities with which defendants here are charged. Even if it did, it would not govern here. Sony involved a construction of the Copyright Act that has been overruled by the later enactment of the DMCA to the extent of any inconsistency between Sony and the new statute."
- What was the court's justification for not applying Sony?

Universal Studios v. Reimerdes

- What about linking?
- Does it mean to provide or otherwise traffic in a violation of the DMCA?
- "[T]he anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it."
- What was the ultimate ruling with regard to linking?

Universal Studios v. Reimerdes

- What about the First Amendment?
- Arguments
  - Computer code is protected free speech
  - DMCA is unconstitutionally overbroad
- Why do both arguments fail?
Universal Studios v. Reimerdes

- What happened after this case?
  - Appeal
  - 321 Studios case

Sony v. GameMasters

- Plaintiff: Sony
- Defendant: Gamemasters
- Civil Action - trademark and copyright infringement, contributory trademark and contributory copyright infringement, violation of the Digital Millennium Copyright Act, and state and federal unfair competition laws.

Sony v. GameMasters

- Plaintiff – Manufactures Sony PlayStation game units, owns various related TMs
- Defendant
  - Video game controller
  - Memory cards
  - Game console moldings
  - CD mechanism boxes
  - Game enhancer devices

The Game Enhancer

- “The Game Enhancer is an external device manufactured by numerous companies which, when plugged into the PlayStation game console, performs at least two functions.”
  - Modify the rules of a specific game.
  - Permit players to play games sold in Japan or Europe and intended by SCEA for use exclusively on Japanese or European PlayStation consoles. The PlayStation console is designed to operate only when encrypted data is read from a CD-ROM that verifies that the CD is an authorized, legitimate SCEA product licensed for distribution in the same geographical territory of the console's sale. Games not licensed for distribution in the same territory as that of the console's sale cannot be played on the PlayStation without a device such as the Game Enhancer.”

Sony v. GameMasters

- “SCEA contends that the Game Enhancer performs a third function: allowing users to play "backups," i.e., counterfeit copies of original PlayStation software. Defendants contend that the Game Enhancer does not enable the console to play counterfeit games. ... The user instructions for the Game Enhancer refer to "Play Imports" but do not in any way refer to "backups" or "bootlegs" or "copies."
- SCEA has submitted advertising from a website for the Game Doctor which suggests that the Game Enhancer 5.0 does in fact enable users to play counterfeit games, but no evidence suggests that GameMasters sold or possessed the Game Enhancer 5.0.

Sony v. GameMasters

- Did Sony win as a matter of law on:
  - contributory copyright, or
  - trademark infringement?
Sony v. GameMasters

- “The Digital Millennium Copyright Act, among other things, prohibits distribution of any product or device which:
  1) is primarily designed or produced for the purpose of circumventing a technological measure (or a protection afforded by a technological measure) that effectively controls access to a system protected by a registered copyright or effectively protects a right of a copyright owner in a registered work or portion thereof;
  2) has only limited commercially significant purpose or use other than to circumvent such a technological measure (or protection afforded it); Or
  3) is marketed for use in circumventing such a technological measure (or protection afforded by it). 17 U.S.C. § 1201(a)(2)-(3) and (b)(1)-(2) (Public Law 105-304, October 28, 1998).”

Sony v. GameMasters

- Section 1201 also prohibits manufacture or distribution of technologies, products and services used to circumvent technological measures which control access. The prohibition applies only if such circumventing technologies are primarily designed for this purpose, have only limited commercial purpose beyond such circumventing purpose, or are marketed for the prohibited purpose. This provision is immediately effective. …"
Lexmark v. Static Control Components

• Who are the parties and what do they do?
  – Lexmark
  – Static Control Components (SCC)

• What are the functions of the programs?
  – Toner Loading Program - calculates toner level in printers manufactured by Lexmark
  – Printer Engine Program - controls various printer functions on Lexmark printers

Background of the Dispute

• “...Lexmark began selling discount toner cartridges for its printers that only Lexmark could refill and that contained a microchip designed to prevent Lexmark printers from functioning with toner cartridges that Lexmark had not re-filled. In an effort to support the market for competing toner cartridges, Static Control Components (SCC) mimicked Lexmark’s computer chip and sold it to companies interested in selling remanufactured toner cartridges.

• “Lexmark brought this action to enjoin the sale of SCC’s computer chips and raise three theories of liability in doing so. Lexmark claimed that
  – SCC’s chip copied the Toner Loading Program in violation of the federal copyright statute.
  – SCC’s chip violated the DMCA by circumventing a technological measure designed to control access to the Toner Loading Program.
  – SCC’s chip violated the DMCA by circumventing a technological measure designed to control access to the Printer Engine Program.”

What is the difference between prebate and nonprebate?

What type of protection did Lexmark obtain on the programs?

Lexmark v. Static Control Components

• What happened at district court?
  “We apply an abuse-of-discretion standard in reviewing a district court’s entry of a preliminary injunction. … A district court abuses its discretion if it relies upon clearly erroneous findings of fact, employs an incorrect legal standard or improperly applies the correct law to the facts. …”

Entitlement to Copyright Protection

• “As this case comes to the court, the parties agree that computer programs may be entitled to copyright protection as ‘literary works’ under 17 U.S.C. §101 and may be protected from infringement under 17 U.S.C. §106. And that is true with respect to a computer program’s object code … and its source code …”
Lexmark v. Static Control Components

• “The parties also agree that Lexmark has registered the Toner Loading Program with the Copyright Office, which is an infringement suit prerequisite, see 17 U.S.C. § 411(a), and which constitutes prima facie evidence of the copyright's validity, see id. §410(c). And the parties agree that SCC shoulders the burden of rebutting the presumptive validity of Lexmark's copyright. …

• “The parties also share common ground when it comes to most of the general principles of copyright infringement applicable to this case…

Lexmark v. Static Control Components

• Even if it is original under 102(a), what about 102(b)?

• “In ascertaining this ‘elusive boundary line’ between idea and expression, between process and non-functional expression, courts have looked to two other staples of copyright law -- the doctrines of merger and scenes a faire.

• “Where the ‘expression is essential to the statement of the idea,’ …. or where there is only one way or very few ways of expressing the idea, …. the idea and expression are said to have ‘merged.’ In these instances, copyright protection does not exist because granting protection to the expressive component of the work necessarily would extend protection to the work’s uncopyrightable ideas as well. …”

Lexmark v. Static Control Components

• “To ‘unlock’ and permit operation of the primary device (i.e., the computer, the game console, the printer, the car), the component must contain either a certain code sequence or be able to respond appropriately to an authentication process. To the extent compatibility requires that a particular code sequence be included in the component device to permit its use, the merger and scenes a faire doctrines generally preclude the code sequence from obtaining copyright protection.

• What did the court find in this case?

Lexmark v. Static Control Components

• “The statute first prohibits the circumvention of “a technological measure that effectively controls access to a work protected [by copyright]” 17 U.S.C. § 1201(a)(1). The statute then prohibits selling devices that circumvent access-control measures:

– No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that:
   (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a copyrighted work;
   (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a copyrighted work;
   (C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing a technological measure that effectively controls access to a copyrighted work.

• Id. § 1201(a)(2). The statute finally bans devices that circumvent “technological measures” protecting “right” of the copyright owner. Id. §1201(b). The last provision prohibits devices aimed at circumventing technological measures that allow some forms of “access” but restrict other uses of the copyrighted work, … such as streaming media, which permits users to view or watch a copyrighted work but prevents them from downloading a permanent copy of the work, …”

Lexmark v. Static Control Components

• The parties also agree that Lexmark has registered the Toner Loading Program with the Copyright Office, which is an infringement suit prerequisite, see 17 U.S.C. § 411(a), and which constitutes prima facie evidence of the copyright's validity, see id. §410(c). And the parties agree that SCC shoulders the burden of rebutting the presumptive validity of Lexmark's copyright. …
Lexmark v. Static Control Components

Reverse Engineering Defenses

• "The statute also contains three "reverse engineering" defenses. A person may circumvent an access control measure "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to [that person]." 17 U.S.C. § 1201(f)(1). A person "may develop and employ technological means" that are "necessary" to enable interoperability. Id. §1201(f)(2). And these technological means may be made available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs." Id. §1201(f)(3). All three defenses apply only when traditional copyright infringement does not occur and only when the challenged actions (in the case of the third provision) would not violate other "applicable laws." ...

Lexmark v. Static Control Components

Distinguish #1

• "In the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution. ... [T]he DMCA applies in [] settings when the product manufacturer prevents all access to the copyrightable material and the alleged infringer responds by marketing a device that circumvents the technological measure designed to guard access to the copyrightable material."

Lexmark v. Static Control Components

Distinguish #2

• "The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, "using" or executing the Printer Engine Program does not in turn create any protected expression. ... And unlike the code underlying video games or DVDs, no encryption or other technological measure prevents access to the Printer Engine Program. Presumably, it is precisely because the Printer Engine Program is not a conduit to protectable expression that explains why Lexmark (or any other printer company) would not block access to the computer software that makes the printer work. Because Lexmark's authentication sequence does not restrict access to this literal code, the DMCA does not apply."

Lexmark v. Static Control Components

• Legislative History

• "Nowhere in its deliberations over the DMCA did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumer goods while leaving the copyrightable content of a work unprotected. ..."

Lexmark v. Static Control Components

• Concurrence – Beware the funny money game!!!

• "We should make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of this case: by, for example, creating a Toner Loading Program that is more complex and "creative " than the one here, or by cutting off other access to the Printer Engine Program. The crucial point is that the DMCA forbids anyone from trafficking in any technology that "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [protected] work." 17 U.S.C. §1201(a)(2)(A) (emphasis added). The key question is the "purpose" of the circumvention technology. The microchip in SCC's toner cartridges is intended not to reap any benefit from the Toner Loading Program - SCC's microchip is not designed to measure toner levels - but only for the purpose of making SCC's competing toner cartridges work with printers manufactured by Lexmark."

Lexmark v. Static Control Components

• What did Lexmark argue in its complaint?

• "... It is not Lexmark's authentication sequence that "controls access" to the Printer Engine Program. See 17 U.S.C. §1201(a)(2). It is the purchase of a Lexmark printer that allows "access" to the program. Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed. ... No security device, in other words, protects access to the Printer Engine Program Code and no security device accordingly must be circumvented to obtain access to that program code."
DMCA Rulemaking

- DMCA Rulemaking has established exemptions since 2000; last one was in 2015
- Rule makings conducted
  - http://copyright.gov/1201/
- Current rulemaking (2015) is located here:

Software Licensing pt. 1

Software Licensing

- Discussion of why software is typically licensed instead of sold
- Differences between negotiated v. non-negotiated contracts

Why license software?

- Licensing software enables a vendor to:
  - Bundle software
  - Price discriminate
  - Control software after resale

Fundamental Issues

- Respective objectives of the parties
- Applicable law to the license

ProCD v. Zeidenberg

- ProCD (P)
  - Compiler of telephone directories
- Zeidenberg (D)
  - Reseller of information from the compiled telephone directories
ProCD v. Zeidenberg

• What is the information that ProCD provides?
• How do users access the information provided by ProCD?
• How did ProCD price its product?
• How were users informed of ProCD’s license agreement?

ProCD v. Zeidenberg

• “Matthew Zeidenberg bought a consumer package of SelectPhone (trademark) in 1994 from a retail outlet in Madison, Wisconsin, but decided to ignore the license. He formed Silken Mountain Web Services, Inc., to resell the information in the SelectPhone (trademark) database.”

ProCD v. Zeidenberg

• “The district court held the licenses ineffectual because their terms do not appear on the outside of the packages. The court added that the second and third licenses stand no different from the first, even though they are identical, because they might have been different, and a purchaser does not agree to--and cannot be bound by--terms that were secret at the time of purchase.”

ProCD v. Zeidenberg

• How was the contract analyzed under the UCC?
  – “What then does the current version of the UCC have to say? We think that the place to start is sec. 2-204(1): ‘A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.’ A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance. And that is what happened.”

ProCD v. Zeidenberg

• “Section 2-606, which defines ‘acceptance of goods’, reinforces this understanding. A buyer accepts goods under sec. 2-606(1)(b) when, after an opportunity to inspect, he fails to make an effective rejection under sec. 2-602(1).”

ProCD v. Zeidenberg

• “Some portions of the UCC impose additional requirements on the way parties agree on terms. A disclaimer of the implied warranty of merchantability must be ‘conspicuous.’ UCC sec. 2-316(2), incorporating UCC sec. 1-201(10). Promises to make firm offers, or to negate oral modifications, must be ‘separately signed.’ UCC secs. 2-205, 2-209(2).”
ProCD v. Zeidenberg

• “Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general (for example, if they violate a rule of positive law, or if they are unconscionable). Because no one argues that the terms of the license at issue here are troublesome, we remand with instructions to enter judgment for the plaintiff.”

Enforceability?

• How enforceable are shrinkwrap agreements?
  – Generally enforceable if terms are reasonable

Clickwrap v. Shrinkwrap

• How do clickwrap license agreements differ from shrinkwrap license agreements?
  – Bits over Internet
  – Terms can be disclosed prior to purchase
• Clickwrap agreements are easier to enforce

Terms of Use

• Are they enforceable?
• Why type of notice must be the user be put on to be enforceable?

Terms of Use

• A web site should contain, in a prominent location, a hyperlink to the Terms and Conditions of Use, to which a user must agree in order to access or use the site. The provisions contained in the Terms and Conditions will vary depending on the type of web site, for example whether the site is “passive” or “active,” whether the site accepts user submissions, and whether the site collects personal information from users.

Specht v. Netscape Communications Corp

• “[W]e are asked to determine whether [plaintiffs], by acting upon defendants’ invitation to download free software made available on defendants’ webpage, agreed to be bound by the software’s license terms (which included the arbitration clause at issue), even though plaintiffs could not have learned of the existence of those terms unless, prior to executing the download, they had scrolled down the webpage to a screen located below the download button.”
Specht v. Netscape Communications Corp

• Nature of underlying dispute - SmartDownload transmitted to defendants private information about plaintiffs' downloading of files from the Internet.

Specht v. Netscape Communications Corp

• "[Certain] plaintiffs acknowledge that when they proceeded to initiate installation of Communicator, they were automatically shown a scrollable text of that program's license agreement and were not permitted to complete the installation until they had clicked on a 'Yes' button to indicate that they accepted all the license terms."

Specht v. Netscape Communications Corp

• Plaintiffs expressly agreed to Communicator's license terms by clicking 'Yes.'

Specht v. Netscape Communications Corp

• If SmartDownload was downloaded, they were not provided with additional license terms.

Specht v. Netscape Communications Corp

• "The sole reference to SmartDownload's license terms on the 'SmartDownload Communicator' webpage was located in text that would have become visible to plaintiffs only if they had scrolled down to the next screen."

Specht v. Netscape Communications Corp

• D.C. – plaintiff's are not subject to the license agreements because they were not provided with sufficient notice.

Specht v. Netscape Communications Corp

• "[W]e conclude that the district court properly decided the question of reasonable notice and objective manifestation of assent as a matter of law on the record before it, and we decline defendants' request to remand for a full trial on that question."

Specht v. Netscape Communications Corp

• "Whether governed by the common law or by Article 2 of the Uniform Commercial Code ('UCC'), a transaction, in order to be a contract, requires a manifestation of agreement between the parties."

Specht v. Netscape Communications Corp

• “Arbitration agreements are no exception to the requirement of manifestation of assent.”
Specht v. Netscape Communications Corp

• “We disagree with the proposition that a reasonably prudent offeree in plaintiffs’ position would necessarily have known or learned of the existence of the SmartDownload license agreement prior to acting, so that plaintiffs may be held to have assented to that agreement with constructive notice of its terms.”

Nguyen v. Barnes & Noble Inc.

• Barnes & Noble appeal of DC denial to compel arbitration against Nguyen pursuant to the arbitration agreement contained in its website’s Terms of Use

Nguyen v. Barnes & Noble Inc.

• Nature of dispute
  – Nguyen purchases 2 touchpads and the orders are cancelled by Barnes & Noble the next day
  – Class action lawsuit

Nguyen v. Barnes & Noble Inc.

• “The website’s Terms of Use are available via a ‘Terms of Use’ hyperlink located in the bottom left-hand corner of every page on the Barnes & Noble website, which appears alongside other hyperlinks labeled ‘NOOK Store Terms,’ ‘Copyright,’ and ‘Privacy Policy.’ These hyperlinks also appear underlined and set in green typeface in the lower lefthand corner of every page in the online checkout process.”
Nguyen v. Barnes & Noble Inc.

- “Because no affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website, the determination of the validity of the browsewrap contract depends on whether the user has actual or constructive knowledge of a website’s terms and conditions.”

- “Courts have consistently enforced browsewrap agreements where the user had actual notice of the agreement.”
- “Courts have also been more willing to find the requisite notice for constructive assent where the browsewrap agreement resembles a clickwrap agreement—that is, where the user is required to affirmatively acknowledge the agreement before proceeding with use of the website.”

- “But where, as here, there is no evidence that the website user had actual knowledge of the agreement, the validity of the browsewrap agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract. … Whether a user has inquiry notice of a browsewrap agreement, in turn, depends on the design and content of the website and the agreement’s webpage. … Where the link to a website’s terms of use is buried at the bottom of the page or tucked away in obscure corners of the website where users are unlikely to see it, courts have refused to enforce the browsewrap agreement.”
- “We therefore hold that where a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice.”

- “[W]e hold that Nguyen did not enter into Barnes & Noble’s agreement to arbitrate.”

Nguyen v. Barnes & Noble Inc.

- “[C]ourts have consistently enforced browsewrap agreements where the user had actual notice of the agreement.”
- “Courts have also been more willing to find the requisite notice for constructive assent where the browsewrap agreement resembles a clickwrap agreement—that is, where the user is required to affirmatively acknowledge the agreement before proceeding with use of the website.”

- “But where, as here, there is no evidence that the website user had actual knowledge of the agreement, the validity of the browsewrap agreement turns on whether the user has actual or constructive knowledge of a website’s terms and conditions.”

- “Courts have also been more willing to find the requisite notice for constructive assent where the browsewrap agreement resembles a clickwrap agreement—that is, where the user is required to affirmatively acknowledge the agreement before proceeding with use of the website.”

- “We therefore hold that where a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice.”

- “[W]e hold that Nguyen did not enter into Barnes & Noble’s agreement to arbitrate.”

Manifestation of Assent

- What could BN have done?
  - Check box accepting terms before proceeding with login
  - Further notice before checkout
  - Better font contrast
Data Security

Victims of Data Breaches

Who are the victims?

- 77% of breaches affected financial organizations
- 24% of breaches occurred in small environments and retail
- 20% of breaches occurred in places involved in manufacturing, transportation, and utilities
- 20% of network/communications and professional services firms
- 38% of breaches impacted large organizations
- 27% affected customers or employees

- Verizon Data Breach Investigations Report 2013

DATA SECURITY BREACH NOTIFICATION STATUTES

CA Data Breach Statute

- “Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expeditious possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.”

States/Federal Government Data Breach Laws

- 47 States and D.C. with breach notification laws
  - Need to understand the differences so that the business can comply with the notification requirements

Breach Law Variations

1) the definition of covered information;
2) the trigger for notification;
3) any exceptions to the law’s notification requirement;
4) a requirement of notification to a state agency or attorney general;
5) the presence or absence of a substantive requirement for data security; and
6) the presence or absence of a private right of action.
Covered Information

• Notice-triggering information (for CA + FL & GA)
• “[F]irst name or initial and last name” and any of the following list of other data: Social Security number; driver’s license number; financial account number plus a password.”
• Since 2013 includes “user names or e-mail addresses in combination with a password or a security question and answer that would permit access to an online account.”

Trigger for Notification

• “[S]tates generally require notification whenever there is a reasonable likelihood that an unauthorized party has ‘acquired’ person information. A minority of states have adopted a higher standard. These states consider whether there is a reasonable likelihood of ‘misuse’ of the information, or ‘material risk’ of harm to the person. The idea is that a breach letter should not be sent to the affected public unless there is a more significant likelihood of harm.”

Notification to State Agency or Attorney General

• “All the breach notification statutes require notification to the affected party. …States that require notice to a state agency or attorney general include Alaska, California, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Maryland, Massachusetts, New York, North Carolina, South Carolina, Vermont, and Virginia.”

Substantive Data Security

• Some states create a substantive duty to take reasonable steps to safeguard data.
• While generally open-ended, the duties generally related to requiring reasonableness in measures taken

Private Right of Action

• Only in a minority of states
• Through a separate statute or under the state’s unfair or deceptive trade practices act.

CIVIL LIABILITY AND STANDING
Pisciotta v. Old National Bancorp

- 7th Cir. 2007
- **Issue**
  - Does ONB owe its users compensation when a hacker used confidential information of its users?
- **History**
  - S.D.IN – no
  - 7th Cir. – affirm

Pisciotta v. Old National Bancorp

- NCR is a hosting facility that maintained the ONB website had a security breach and notified ONB
- ONB notified its customers of the security breach

Pisciotta v. Old National Bancorp

- P do not allege direct financial loss or being the victim of an identity theft
- “The plaintiffs requested ‘[c]ompensation for all economic and emotional damages suffered as a result of the Defendants’ acts which were negligent, in breach of implied contract or in breach of contract,’ and ‘[a]ny and all other legal and/or equitable relief to which Plaintiffs . . . are entitled, including establishing an economic monitoring procedure to insure [sic] prompt notice to Plaintiffs . . . of any attempt to use their confidential personal information stolen from the Defendants.’”

Pisciotta v. Old National Bancorp

- “As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant’s actions. We concur in this view.”

Pisciotta v. Old National Bancorp

- “The provisions of the statute applicable to private entities storing personal information require only that a database owner disclose a security breach to potentially affected consumers; they do not require the database owner to take any other affirmative act in the wake of a breach. If the database owner fails to comply with the only affirmative duty imposed by the statute — the duty to disclose — the statute provides for enforcement only by the Attorney General of Indiana. It creates no private right of action against the database owner by an affected customer. It imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow. …”

Future Risk of Harm=Standing?

- “[A] number of courts have had occasion to decide whether the “risk of future harm” posed by data security breaches confers standing on persons whose information may have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative. … Here, no evidence suggests that the data has been—or will ever be—misused. The present test is actuality, not hypothetical speculations concerning the possibility of future injury. Appellants’ allegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing.”
  - Reilly v. Ceridian Corp. (3rd. Cir. 2011)
Resnick v. AvMed

- 11th Cir. 2012
- Issue
  - Liability for a data breach

Two laptop computers stolen from AvMed’s office
- “AvMed did not take care to secure these laptops, so when they were stolen the information was readily accessible. The laptops were sold to an individual with a history of dealing in stolen property. The unencrypted laptops contained the sensitive information of approximately 1.2 million current and former AvMed members.”

Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes an injury in fact under the law.

“Generally, to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence. … Here, Plaintiffs allege a nexus between the two events that includes more than a coincidence of time and sequence: they allege that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs’ identity. Plaintiffs explicitly make this connection when they allege that Curry’s identity was stolen by changing her address and that Moore’s identity was stolen by opening an E*Trade Financial account in his name…”

Plaintiffs have sufficiently alleged a nexus between the data theft and the identity theft and therefore meet the federal pleading standards. Because their contention that the data breach caused the identity theft is plausible under the facts pled, Plaintiffs meet the pleading standards for their allegations on the counts of negligence, negligence per se, breach of fiduciary duty, breach of contract, breach of implied contract, and breach of the implied covenant of good faith and fair dealing. …

Arguments have generally been dismissed

Data Breach Theories of Harm

- “(1) The exposure of their data has caused them emotional distress;
  (2) The exposure of their data has subjected them to an increased risk of harm from identity theft, fraud, or other injury; or
  (3) The exposure of their data has resulted in their having to expend time and money to prevent future fraud, such as signing up for credit monitoring, contacting credit reporting agencies and placing fraud alerts on their accounts, and so on.”
- Arguments have generally been dismissed
**FTC REGULATION**

**Enforcement Actions**

- “The FTC's initial enforcement actions for data security involved companies that failed to live up to promises made about data security in their privacy policies. The FTC has deemed the failure to follow statements made in a privacy policy to be a deceptive act or practice. A deceptive act or practice is a material ‘representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer’s detriment.’

**Unfair Data Security Practices**

- “Under the FTC Act, a practice is unfair if it ‘causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition.’ 15 U.S.C. §45(n).”

**Section 5**

- Violation of a consent decree results in fines
- Can issue fines under other sections
- FTC can obtain injunctive relief
- No private right of action

**FTC v. Wyndham Worldwide Corp.**

- 3rd Circuit 2015
- Issue
  - Does the FTC have authority to regulate cyberspace and its Wyndham under fair notice?

**FTC v. Wyndham Worldwide Corp.**

- Wyndham
  - Hotel company
  - Operates a property management system and computer network
FTC v. Wyndham Worldwide Corp.

• "The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, ‘taken together, unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.’"

FTC v. Wyndham Worldwide Corp.

• What were Wyndham’s failures?
  – Stored payment card info in clear text
  – Easily guessed passwords
  – Failed to use readily available security measures (e.g., firewalls)
  – Failed to take adequate precautions with company and vendor connecting computers
  – Failed to employ reasonable measures to detect and prevent unauthorized access or conduct security investigations
  – Did not follow proper incident response procedures

FTC v. Wyndham Worldwide Corp.

• Overstated privacy policy
  • "The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data.”

FTC v. Wyndham Worldwide Corp.

• Cybersecurity attacks
  – 3 occasions in 2008 and 2009
  – 1st LAN access through a hotel, brute force guessing IDs and passwords, accessed an admin account, obtain unencrypted consumer data on 500K accounts, information sent to Russia
  – 2nd attached through admin account; Wyndham unaware until consumer complaints over fraud charges, memory-scraping malware on computers; obtained payment card info for 50K users
  – 3rd attack access to property management servers allowed obtain card information for 69K users
  – Payment card info for a total of 619K consumers, 10.6 million in fraud loss, and other consumer injuries
**FTC v. Wyndham Worldwide Corp.**

- “Unfair methods of competition in commerce” was meant by Congress to be flexible and evolving
- Language evolved to “unfair methods of competition in or affecting commerce”

**FTC v. Wyndham Worldwide Corp.**

- §45(n) – “The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.”

**FTC v. Wyndham Worldwide Corp.**

- “A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.”

**FTC v. Wyndham Worldwide Corp.**

- “For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks.”

**FTC v. Wyndham Worldwide Corp.**

- Three Governing factors
  1) Offends public policy
  2) Immoral, unethical, oppressive, or unscrupulous,
  3) Causes substantial injury to consumers, competitors, and/or other businessmen
FTC v. Wyndham Worldwide Corp.

• “Subsection 45(n) asks whether ‘the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.’ While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis, … that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.’

128

FTC v. Wyndham Worldwide Corp.

• “Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.”

129

FTC v. Wyndham Worldwide Corp.

• “Wyndham’s as-applied challenge falls well short given the allegations in the FTC’s complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used weak firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use any firewall at critical network points, [] did not restrict specific IP addresses at all, [] did not use any encryption for certain customer files, id. [] and did not require some users to change their default or factory-setting passwords at all[]. Wyndham did not respond to this argument in its reply brief.”

130

Program Completed

All course materials - Copyright 2000-16 Randy L. Canis, Esq.