Computers and the Law

Randy Canis

CLASS 12

DMCA pt. 2;
Software Licensing pt. 2;
Privacy
Part 2

- Limitations on liability relating to material online §512

Background of “Hypothetical Dispute”

- CS317-ISP (i.e., the client) recently provided us (client’s counsel) with an e-mail it received from NetPD (enforcer of copyrights). In the e-mail, NetPD advised CS317-ISP that a digital audio file in which one of its clients (computer user) has rights was located on one of CS317-ISP’s servers and that the e-mail should be construed as notice under the Digital Millennium Copyright Act ("DMCA") and requested that certain actions should be taken by CS317-ISP. We have been asked by CS317-ISP to determine how it should respond to this message.
ISPs and the DMCA

• Internet Service Providers (ISPs) are concerned with their liability for subscribers who use their resources to commit unlawful acts. The greatest concern has been liability for copyright infringement, as their users transmit a vast amount of material through the Internet and it is impractical to screen out infringing material. The law was unprepared for the wealth and speed of material available on the Internet and, as a result, legal reform was necessary to protect ISPs from liability from actions taken by their subscribers.

ISPs and the DMCA

• Congress responded to the plight of ISPs by introducing legislation that would provide them with "safe harbors" (i.e., exemptions) that would shield them from liability in certain circumstances. In 1998, the Online Copyright Infringement Liability Limitation Act (OCILLA) was signed into law as part of the Digital Millennium Copyright Act and provided safe harbors to protect ISPs in four distinct circumstances: (a) transitory digital network communications, (b) system caching, (c) information residing on systems or networks at direction of users, and (d) information location tools. OCILLA was written into law as 17 U.S.C. §512, which appears in its entirety in the Appendix.

Prerequisites

Introduction

• Various prerequisites are necessary for ISPs to take advantage of some of the safe harbors including designating an agent with the Copyright Office to receive service, receiving sufficient notice from a copyright owner to react in the prescribed statutory manner, complying with standard technical measures, and having an anti-infringement policy in effect. Below we determine whether or not CS317-ISP has met the prerequisites to take advantage of any safe harbors.
Prerequisites

Designated Agent

- CS317-ISP must have registered a designated agent with the Copyright Office pursuant to §512(c)(2) to take advantage of the safe harbor for information residing on systems or networks at direction of users (i.e., §512(c)). We have reviewed the Service Provider Agent List at the Copyright Office and CS317-ISP is not listed.
- Without designating an agent, CS317-ISP is unable to receive the exemption for information residing on systems or networks at direction of users with the present matter. However, as will be further explained below, this exemption is immaterial with respect to the present notice received from NetPD as the notice relates to the exemption for transitory digital network communications (i.e., §512(a)).

Prerequisites

- CS317-ISP should authorize our firm to immediately file with the Copyright Office the form necessary to designate our firm as the Designated Agent on its behalf.
- Further, it is also necessary to modify CS317-ISP's Internet Service Acceptable Use Policy (AUP) to provide the name, address, phone number, and electronic mail address of our firm as its Designated Agent for receiving notice.
- Thereafter, in the future CS317-ISP will be eligible to receive the exemption for information residing on systems or networks at direction of users. See Exhibit 3 for our proposed modification to the AUP.

Prerequisites

Sufficiency of Notice Provided by NetPD

- The e-mail received from NetPD states that its letter "constitutes notice to [CS317-ISP] that [the indicated] site operator maybe be liable for the infringing activity occurring on [CS317-ISP's] server." Therefore, we consider the implications of the e-mail and whether (i) CS317-ISP has received "sufficient notice" such it will be deemed to have knowledge of infringing material on its system, and (ii) the effect, if any, of receiving actual knowledge of the infringing material on its system.
Prerequisites

- Under the exemption for transitory digital network communications, knowledge is not taken into consideration. However, the notice may be considered knowledge under 512(i)(1)(A) that the user committed an infringement, and that should multiple notices be issued on the same user for violating copyrights than that user should be consider a repeat infringer and reprimanded accordingly. (See Prerequisite D below for more information regarding repeat infringers.)

Prerequisites

CS317-ISP Must Not Interfere with Standard Technical Measures

- Pursuant to §512(i)(1)(B), CS317-ISP must accommodate and not interfere with "standard technical measures". In the future, it is intended that standard technical measures will be used by copyright owners to identify or protect their copyrighted works. However, this is not at issue at the present time because there is yet to be a standard means for protecting copyrighted works. We should re-evaluate this factor when there is a general consensus as to what are standard technical measures.

Prerequisites

CS317-ISP Must Have an Anti-Infringement Policy in Effect

- For CS317-ISP to use the OCILLA exemptions, under §512(i)(1)(A) it must have adopted and reasonably implemented "a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." We are unaware of how CS317-ISP informs its subscribers and account holders of its AUP.
Prerequisites

• Next, we consider whether CS317-ISP's AUP complies with the requirements of OCILLA. Sections 8.1 of the AUP allow CS317-ISP to "deny [a] [s]ubscriber access to all or part of [CS317-ISP's] service without notice if [a] [s]ubscriber engages in any conduct or activities that [CS317-ISP] in its sole discretion believes violates any of the terms and conditions in this AUP.
• Thus, pursuant to Section 8.1, CS317-ISP can terminate a subscriber who, according to Section 1.1, "posts, transmits, re-transmits or stores material on or through [the CS317-ISP] system services or products that: (i) is in violation of any local, state, federal or non-United law or regulation; (ii) threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, "Persons"); or (iii) violates the rights of any person including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by [a] [s]ubscriber." Therefore, it appears as though CS317-ISP has met the anti-infringement requirement.

Prerequisites

• However, CS317-ISP should adopt the following means of notifying its subscribers of the AUP:
  1. E-mail subscribers when the AUP has been modified;
  2. Create a version number and last updated date for the AUP so subscribers who view the AUP online will know whether it has changed since the last time they reviewed it;
  3. Provide a link to the AUP on an easily locatable section of the website (e.g., such as the front page of the website); and
  4. Make sure that before users gain access to CS317-ISP's system (i.e., by becoming subscribers) that they agree to the AUP such as through a click wrap agreement.
• By following steps 1-4 above, CS317-ISP will more clearly comply with this prerequisite as well as follow better Internet practices by effectively alerting its subscribers of its policies currently in effect.

Action Necessitating Need for DMCA Safe Harbor(s)

• In its e-mail, NetPD indicates that one of CS317-ISP's subscribers has transferred a copyrighted MP3 digital audio file using Aimster, and that the copyright owner has given NetPD the rights to enforce its copyright.
• NetPD has requested that CS317-ISP take action including that it (i) remove the site or delete the infringing sound files or that it disable access to the disclosed site or the infringing files being offered via its system, (ii) inform the subscriber of the illegality of his or her conduct, and (iii) confirm with NetPD that the infringing activity has ceased.
• We will determine what liability CS317-ISP has for providing and continuing to provide service to this subscriber, what actions can and should be taken by CS317-ISP to avoid liability and lawsuits, and how CS317-ISP should respond to the specific request made by NetPD.
Summary of the Safe Harbors

- OCILLA provides safe harbors to ISPs in four distinct circumstances: transitory digital network communications (i.e., 512(a)), system caching (i.e., 512(b)), information residing on systems or networks at direction of users (i.e., 512(c)), and information location tools (i.e., 512(d)). It is not necessary to obtain all four safe harbors to avoid liability.
- Rather, when the behavior of an ISP falls within a particular safe harbor, that behavior will be exempted harbor if the ISP meets the prerequisites for obtaining the safe harbor as well as the particular requirements of the specific safe harbor.
- Below we review whether CS317-ISP’s behavior falls within any of the safe harbors and whether the safe harbors are met.

SAFE HARBOR 512(a): Transitory Digital Network Communications

Background

- As discussed above, CS317-ISP has met the prerequisites to take advantage of the safe harbor for transitory digital network communications. We must consider whether the complained of behavior falls within this particular exemption for transitory digital network communications, and whether CS317-ISP has met the requirements to take advantage of this exemption.

SAFE HARBOR 512(a): Transitory Digital Network Communications

Requirement #1: CS317-ISP Must Be A “Service Provider”

- The first requirement for CS317-ISP to qualify as a "service provider" under 512(k)(1)(A) is that it must be an "entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received." CS317-ISP provides the services listed above and is a service provider with respect to this exemption.
SAFE HARBOR 512(a): Transitory Digital Network Communications

Requirement #2: Transmission of Material Through CS317-ISP’s System

- The second requirement for CS317-ISP to fall within the transitory digital network communications exemption is that its subscriber’s behavior must stem from CS317-ISP providing services for the “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections.” With respect to the message received from NetPD, the subscriber was using CS317-ISP’s Internet Access to connect to the Internet and thus was “provided a connection” by CS317-ISP. The subscriber transferred the MP3 file by using its connection provided by CS317-ISP. Therefore, CS317-ISP’s relation to the subscriber’s behavior falls within this exemption.

Requirement #3: Transmission Must Be Eligible

- The third and final requirement for CS317-ISP to obtain the transitory digital network communications exemption is that the “transmission” sent by CS317-ISP’s subscriber must be eligible, such that CS317-ISP did not take part in the selective transmission of the file.
  - Specifically, the transmission must meet the following five elements of §512(a): (1) the transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (5) the material is transmitted through the system or network without modification of its content.

- With respect to the action complained of by NetPD, the use of Aimster and the transmission of the sound file was initiated by the subscriber and not by CS317-ISP. The subscriber was connected to CS317-ISP’s system and the Internet through a standard automated process. CS317-ISP did not direct the subscriber to whom it could provide its information (including the MP3 file). Further, CS317-ISP does not maintain a copy of material made in intermediate or transient storage in a manner that is ordinarily accessible to anyone beyond the anticipated recipients, nor does it maintain a copy of material on its system for a longer period than is reasonably necessary for a transmission. Finally, the material is transmitted through CS317-ISP’s system without modification. Therefore, CS317-ISP has complied with the above five elements with this respect to the transmission of the allegedly infringing MP3 file.
SAFE HARBOR 512(a): Transitory Digital Network Communications

**Safe Harbor is Met**
- CS317-ISP has met the necessary requirements of the transitory digital network communications exemption because it is a service provider, the material was transmitted through its system and the transmission is eligible. Therefore, CS317-ISP is not liable for monetary relief (including without limitation damages, costs and attorneys’ fees) for the actions taken by its subscriber while using Aimster.

SAFE HARBOR 512(b): System Caching

**Background**
- The second safe harbor (i.e., 512(b)) is for “system caching” and limits the liability for copyright infringement of a service provider by reason of the immediate and temporary storage of material on a system or network controlled or operated by or for the service provider..."

SAFE HARBOR 512(b): System Caching

**Safe Harbor is Not Relevant**
- NetPD has not complained about CS317-ISP’s system caching but rather has complained of the behavior of a CS317-ISP subscriber with respect to one of its copyrighted MP3 digital audio files. Thus, as CS317-ISP’s behavior does not fall within this safe harbor, this exemption will not shield CS317-ISP from liability from the complained of activity and therefore will not be further considered herein. However, we recommend that CS317-ISP provide us with a written description of its policy of system caching so that we can compare it against this exemption as a prophylactic measure against a possible future system caching complaint.
SAFE HARBOR 512(c): Information Residing on Systems or Networks at Direction of Users

• **Background**
  • The third and penultimate safe harbor (i.e., 512(c)) limits the liability for copyright infringement for the storage of infringing material at the direction of a user on a system or network controlled by the service provider.

SAFE HARBOR 512(c): Information Residing on Systems or Networks at Direction of Users

**Safe Harbor is Not Relevant**

• NetPD's message seems to complain of a file stored on CS317-ISP system. However, as outlined above, the file was not stored on CS317-ISP's system but was rather transferred through CS317-ISP's system. Therefore, the exemption for information residing on systems or networks at direction of users is not relevant to the message received from NetPD.

SAFE HARBOR 512(c): Information Residing on Systems or Networks at Direction of Users

**Important Safe Harbor Note**

• A future analysis under 512(c) will be vastly different from 512(a) and it will be necessary to prepare a different response to both the subscriber and the copyright owner. CS317-ISP should consider providing us with a copy of any such notices it receives so that we can make a determination as to what action should be taken.
SAFE HARBOR 512(d): Information Location Tools

Background

• The fourth and final safe harbor (i.e., 512(d)) is for "information location tools" and limits the liability for copyright infringement of a service provider by reason of it "referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link."

SAFE HARBOR 512(d): Information Location Tools

Safe Harbor is Not Relevant

• NetPD has not complained of the links on CS317-ISP's website but rather has complained of the behavior of a CS317-ISP subscriber with respect to one of its copyrighted MP3 digital audio files. Thus, as CS317-ISP's behavior does not fall within this safe harbor, this exemption will not shield CS317-ISP from liability from the complained of activity and therefore will not be further considered herein.

Injunctive Relief for NetPD

• We have concluded that under the exemption for transitory digital network communications, CS317-ISP is not monetarily liable for the behavior of CS317-ISP's subscriber. However, we have not addressed the issue of injunctive relief.
• Under §502 of the Copyright Act, courts can grant temporary and final injunctions to prevent or restrain infringement of copyrights. However, §512(j)(6) of the DMCA limits the injunctive relief available to copyright owners when a service provider qualifies for the transitory digital network communications exemption.
• With appropriate court action, NetPD could potentially obtain an order restraining CS317-ISP from providing access to the subscriber who transmitted the infringing file by ordering CS317-ISP to terminate its subscriber's account.
• Therefore, if CS317-ISP refuses to comply with NetPD's demands, NetPD could take CS317-ISP to court to force the termination of the subscriber's Internet access.
Receiving Subpoena from NetPD

• Under §512(h), NetPD could request a district court to issue a subpoena to CS317-ISP to identify an alleged infringer. Should CS317-ISP receive such a subpoena, it will need to expeditiously disclose to NetPD the information required by the subpoena. If CS317-ISP receives such a notice, it should contact us immediately.

CS317-ISP’s Actions Against the Subscriber

Determine the Identity of the Subscriber

• CS317-ISP should review the necessary information such as server logs to determine the subscriber responsible for transferring the allegedly infringing file. If the subscriber can be identified, this subscriber’s account information and the notice received from the copyright owner should be stored in a special file and retained indefinitely.

CS317-ISP’s Actions Against the Subscriber

Provide the Subscriber With Notice

• Once the subscriber is identified, CS317-ISP should send a warning notice to the subscriber advising him or her of the message received from NetPD. While it is not mandatory to provide notice to the infringer, it will be good practice to do since CS317-ISP has a policy of terminating repeat infringers. We have provided a notice for CS317-ISP to send the infringer and it is included herewith as Exhibit 1.
CS317-ISP's Actions Against the Subscriber

Future Infringement by the Subscriber

• We propose the following plan for reprimanding "repeat infringers": If the subscriber is cited a third time for copyright infringement within a twelve month period, CS317-ISP should suspend the subscriber’s account for a period of thirty days. If the subscriber is cited a fourth time for copyright infringement during a twelve-month period, the subscriber’s account should be terminated and the subscriber should be permanently banned from CS317-ISP’s system.

• We recommend that CS317-ISP adopt the above-mentioned plan or something similar to it for reprimanding repeat infringers. If CS317-ISP does not take significant action against subscribers who are repeat infringers, under §512(i)(1)(A) it could lose its ability to take advantage of the safe harbors contained in §512.

CS317-ISP’s Response to NetPD

• As previously mentioned, NetPD has requested that CS317-ISP take action including that it (i) remove the site or delete the infringing sound files or that it disable access to the subscriber’s site or the infringing files being offered via your system, (ii) inform the subscriber of the illegality of his or her conduct, and (iii) confirm with NetPD that the infringing activity has ceased.

• With respect to the first request, CS317-ISP cannot remove the site, delete the infringing sound file, or disable access to the subscriber’s site or the infringing MP3 file being offered via CS317-ISP’s system because the MP3 file was a transient file and only was available through CS317-ISP’s due to the nature of the subscriber accessing the Internet and transferring the file through its Internet connection and use of the Aimster protocol. Therefore, it is impossible to comply with NetPD’s first request.

• With respect to the second request, CS317-ISP can confirm that it has notified the subscriber of its infringing activity. Finally, with respect to the third request, CS317-ISP should not confirm cessation of the subscriber’s infringing activity because doing so may suggest some control over the subscriber and its actions when there is no such duty.

Conclusion

• We believe under the safe harbor for transitory digital network communications (i.e., §512(a)) that CS317-ISP is not liable for the behavior of one of its subscribers with respect to his or her transferring of a digital MP3 sound file using the Aimster protocol. We have also prepared a warning notice for CS317-ISP to send to the infringer, along with a proposed response that we wish to send on CS317-ISP’s behalf to NetPD.

With respect to future notices received by copyrights owners, we strongly urge CS317-ISP to provide us with a copy of the notice received so that we determine an appropriate response.
Conclusion

• Further, as discussed above, CS317-ISP should authorize our firm to immediately submit to the Copyright Office the filing necessary to designate our firm as the Designated Agent on its behalf. Finally, we have enclosed a proposed modification to your AUP to comply with Designated Agent requirements.

UMG v. Shelter Capital Partners

• Veoh
  – website that enables users to share videos
  – implemented various procedures to prevent copyright infringement through its system
• Universal Music Group (UMG)
  – recorded music and music publishing

UMG v. Shelter Capital Partners

• Background
  – users in the past have downloaded videos without UMG’s authorization that include UMG songs
  – UMG sued for direct and secondary copyright infringement
  – DC ruled in favor of Veoh under DMCA 512(c)
UMG v. Shelter Capital Partners

• How does Veoh work?
  – View videos uploaded by users and partner content
  – Content viewed through standalone software application or Veoh website
  – Veoh makes money through advertising
• What kind of agreements must the User agree to before sharing material?

UMG v. Shelter Capital Partners

• What happens when a video is uploaded?
  – transcoding
  – extraction of metadata
  – assignment of a web address
• Do Veoh employees review videos before they are made publicly available?

UMG v. Shelter Capital Partners

• How are videos made available?
  – streaming
  – downloading
• How is copyright infringement automatically prevented?
  – hash filtering
  – audio fingerprinting
• Veoh filtered backlog of content with audio fingerprinting and removed 60K files
UMG v. Shelter Capital Partners

• Who else did UMG sue?
  – Three of Veoh’s investors as defendants on theories of secondary liability

UMG v. Shelter Capital Partners

• 512(c)
  (1) In general. — A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider

UMG v. Shelter Capital Partners

• (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
• (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
• (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
UMG v. Shelter Capital Partners

- (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
- (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

UMG v. Shelter Capital Partners

- What are UMG’s arguments?
  1. the alleged infringing activities do not fall within the plain meaning of “infringement of copyright by reason of the storage [of material] at the direction of a user”
  2. genuine issues of fact remain about whether Veoh had actual knowledge of infringement, or was “aware of facts or circumstances from which infringing activity [wa]s apparent”
  3. Veoh “receive[d] a financial benefit directly attributable to . . . infringing activity” that it had the right and ability to control under § 512(c)(1)(B).

UMG v. Shelter Capital Partners

- Do the functions of Veoh's software destroy storage at the direction of users?
  - No, because by reason of storage and the infringer does not have to conduct the storage
  - “We hold that the language and structure of the statute, as well as the legislative intent that motivated its enactment, clarify that § 512(c) encompasses the access-facilitating processes that automatically occur when a user uploads a video to Veoh.”
UMG v. Shelter Capital Partners

- What about actual knowledge?
  - UMG argues that Veoh had knowledge or awareness of other infringing videos that it did not remove
  - UMG failed to rebut Veoh’s showing “that when it did acquire knowledge of allegedly infringing material — whether from DMCA notices, informal notices, or other means — it expeditiously removed such material.”
  - “We therefore hold that merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one’s services could be used to share infringing material, is insufficient to meet the actual knowledge requirement under § 512(c)(1)(A)(i).”
  - “[W]e hold that Veoh’s general knowledge that it hosted copyrightable material and that its services could be used for infringement is insufficient to constitute a red flag.

- What about financial benefit directly attributable to an infringing activity?
  - “[W]e hold that the “right and ability to control” under § 512(c) requires control over specific infringing activity the provider knows about. A service provider’s general right and ability to remove materials from its services is, alone, insufficient. Of course, a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge.”

Software Licensing pt. 2
Why License Intellectual Property?

- Intellectual property provides owner with exclusive rights
- A license enables the owner to provide permission, in the form of a license, to another party to utilize certain exclusive rights
- Without a license, the other party would infringe certain intellectual property rights of the owner

Applicable Legal Areas to Licensing Law

- Contract Law
  - Common Law
  - Uniform Commercial Code (UCC) Article 2
- Intellectual Property Law
- Antitrust, Misuse, and Preemption

Agreement Structure

- Let’s look at the structure of an agreement
Parties, Effective Date, and “Agreement”

• The First Paragraph
  – Identifies the parties to the agreement;
  – Sets out the “effective date” of the agreement (i.e., when the term of the agreement begins);
  – Probably defines the word “Agreement”

Effective Date

• When does the agreement come into effect?
• Past date, date of signing, future date?

Parties

• Who is entering into the agreement?
• Is your agreement with a corporate entity, an individual, or both?
Recitals

• The “whereas” is typically set apart in capital letters and/or bold text;
• Defines the nature of the parties businesses;
• Defines the background of the parties agreement;
• Links the nature and background to the culmination of the agreement

After the Recitals

• After the “whereas” clauses there is a transitioning sentence that starts “now, therefore…”;
• The section containing the definitions (if applicable) is typically first (although at times may be a later section or an exhibit);
• The second section of the agreement usually gets to the meat of the agreement by containing the service(s) to be provided or the good(s) to be delivered;
• The last section of the agreement usually contains a series of general clauses;
• The agreement has signature blocks for the parties that are executing the agreement and states not only the persons signing the agreement but the capacity in which they are signing the agreement.

Definitions

• Capitalized words should only be words that are defined in the agreement.
• Defined terms are either defined at the first instance in the text of the agreement or in a definition section either after the recitals, at the end of the agreement, or in an exhibit/appendix
License Grant

• What rights are being granted under the license agreement?
  – Copyrights, patents, trademarks, trade secrets, right of publicity, data/information
• What conditions are associated with the license?
  – Areas covered
  – Exclusive v. Non-Exclusive
  – Transferable?

Length and Scope of Grant

• **Perpetual** – rights run continuously so long as the right exists
• **Irrevocable** – not cancelable by the licensor for any reason
• **Royalty Free** – licensee does not owe any money to obtain the benefit of the license
• **Fully Paid Up** – all money due has been paid, and no more money is owed

Delivery, Inspection, and Acceptance

• The agreement should address how and when project deliverables are to be provided to the client, how the deliverables may be inspected, the procedures that are to be followed for the client to accept the deliverables, and what the developer’s obligations will be if a deliverable is rejected.
Delivery

- **When** something must be delivered
- **How** something must be delivered
- **Where** something must be delivered

Inspection

- Inspection means evaluating a deliverable for acceptance or rejection
- Agreement should specify how inspection should occur and the time for the inspection to occur

Acceptance

- Acceptance defines the criteria and manner for accepting deliverables
- May require a particular form of acceptance
- Could include failing to reject within a prescribed period of time
Rejection

- Process for rejecting a deliverable should also be described
  - Is the rejection automatic if not expressly accepted during a particular time period?
  - Is there a process to rejection and then for the developer to submit for reacceptance?

Consideration

- Payment or other consideration may include:
  - Payment of money (royalties)
  - Services
  - A license (reciprocal license)

Duration

- How long will the agreement run?
  - Initial term and renewal term(s)
    - Is the renewal term auto-renew such that one of the parties need to opt prior to a certain date for the auto-renewal not to occur?
  - Limited duration, unlimited duration, or an unspecified duration
    - Term with automatic renewals
### Agreement Termination

- Notice of termination
  - Form and timing for termination
- Cancellation
  - Material breach
- Additional obligations post cancellation or termination

### Audit and Accounting Rights

- Should records be maintained by the licensor and available for inspection from time to time by licensee?
- What happens if the audit determines that there is an underpayment, underperformance, and the like?
  - Financial penalty?

### Limitation of Liability

- “NEITHER PARTY SHALLE BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES THAT ARISE OUT OF OR RELATED TO THE AGREEMENT, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.”
**Damages**

- **Direct damages** – unpaid fees or consideration received by the breaching party but never paid
- **Incidental damages** – reasonable charges, expenses, or commission incurred incident to a breach
- **Consequential damages** – “any loss of anticipated benefits resulting from the inability to use the licensed material or intellectual property of which the breaching party, at the time of contracting, had reason to know and could not be reasonably prevented.”

**Warranties**

- What is the expectation of what one party is warranting will happen or is true?
- **Implied Warranties**
  - Merchantability
  - Goods will fit for a particular purpose
  - Automatically part of a contract unless disclaimed

**Warranty Disclaimer**

- LICENSOR DISCLAIMS ALL OTHER WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Indemnification
• Reimbursement for breach of a warranty
• Ability to pay and/or insurance?

Choice of Law/Forum
• Choice of Law
  – What jurisdiction's legal rules apply to a transaction?
  – "Jurisdiction with the most significant relationship to the transaction or inquiry in question and to apply the law of that jurisdiction"

Choice of Law/Forum
• Developer
  – This Agreement shall be governed in all respects by the laws of the State of California without regard to its conflict of laws provisions, and Client and Developer agree that the sole venue and jurisdiction for disputes arising from this Agreement shall be the appropriate state or federal court located in the City of San Jose, and Client and Developer hereby submit to the jurisdiction of such courts.
Choice of Law/Forum

- **Client**
  - This Agreement shall be governed and interpreted in accordance with the laws of the state of __________ without regard to principles of conflict of laws. The Parties agree to submit to the exclusive jurisdiction over all disputes hereunder or related hereto in the federal and state courts in the State of __________ located in __________ County.

Time is of the Essence

- **Seller** recognizes that time is of the essence in this Agreement and that the failure to develop, test and deliver the deliverables hereunder in accordance with the Delivery Schedule shall result in expense and irreparable damage to Buyer.

Force Majeure

- **Developer**
  - Except for the payment of fees by Client, if the performance of any part of this Agreement by either party is prevented, hindered, delayed or otherwise made impracticable by reason of any flood, riot, fire, judicial or governmental action, labor disputes, act of God or any other causes beyond the control of either party, that party shall be excused from such to the extent that it is prevented, hindered or delayed by such causes.
Force Majeure

• Client
  – Nether Party shall be deemed in default of this Agreement to the extent that performance of its obligations or attempts to cure any breach are delayed, restricted or prevented by reason of any act of God, fire, natural disaster, act of government, strikes or labor disputes, inability to provide raw materials, power or supplies, or any other act or condition beyond the reasonable control of the party in question.

Unconscionability

• If license terms of an agreement is unconscionable, a court can potentially:
  – Strike down the entire agreement
  – Strike down an applicable portion of the agreement (severability)
  – Rewrite an applicable portion of the agreement (blue pencil)

Severability

• Developer
  – If any provision of this Agreement is determined to be invalid under any applicable statute or rule of law, it is to that extent to be deemed omitted, and the balance of the Agreement shall remain enforceable.

• Client
  – Should any provision of this Agreement be held to be void, invalid or inoperative, the remaining provisions of this Agreement shall not be affected and shall continue in effect and the invalid provision shall be deemed modified to the least degree necessary to remedy such invalidity.
Waiver

• The failure of either Party to partially or fully exercise any right or the waiver by either party of any breach, shall not prevent a subsequent exercise of such right or be deemed a waiver of any subsequent breach of the same or any other term of this Agreement.

Entire Agreement

• This Agreement, including the Schedules hereto, sets forth the entire agreement between the Parties on this subject and supersedes all prior negotiations, understandings and agreements between the Parties concerning the subject matter. No amendment or modification of this Agreement shall be made except by a writing signed by the Party to be bound thereby or the successor or assign of such Party.

Assignability

• Can on or other assign rights under the contract to another party?
  – With or without consent?
  – Not to be unreasonably withheld?
  – In the event of a merger or acquisition?
Notices

- Where should notices be sent?
- To whom should the notices be sent?
- What method should the notices be sent?
  - Fax, certified mail

Who Owns the Developments?

- Work made for hire
- Discussed during copyright law
- Advantages of having ownership addressed in the agreements

Privacy
Privacy Policies

• Part of self-regulation
• “[Privacy] policies describe the information that is collected, how it will be used and shared, and how it will be safeguarded. Consumers are sometimes offered a choice to opt-out of some uses of their data.”

FTC’s View

• “Since the late 1990s, the Federal Trade Commission (FTC) has deemed violations of privacy policies to be an ‘unfair or deceptive’ practice under the FTC Act. The FTC has the power to enforce the FTC Act. The result of the FTC’s involvement has been to create a system of quasi-self-regulation, where companies define the substantive terms of how they will collect, use, and disclose personal data, but they are then held accountable to these terms by the FTC. Over time, however, the FTC has interpreted the FTC Act as requiring more of companies than merely following promises.”

Compliance and Strategy

• “Compliance means developing safeguards, including training the workforce, to make sure that the company follows all privacy and security laws and regulations. Strategic thinking means assessing privacy risks, training the workforce about privacy awareness, helping to shape products and services so that they minimize any potential privacy concerns, and stopping or limiting a company’s actions that consumers might find too privacy-invasive.”
FTC Section 5 Enforcement

• “Since the mid-1990s, the Federal Trade Commission (FTC) has used Section 5 of the FTC Act to regulate consumer privacy. Section 5 prohibits ‘unfair or deceptive acts or practices in or affecting commerce.’ 15 U.S.C. §45. The FTC views violations of privacy policies as a ‘deceptive’ practice.”

Deception under the FTC

• “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.’”

Unfairness under the FTC

• “The FTC Act classifies a trade practice as 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). Actions of a company can be both deceptive and unfair.”
In the Matter of Snapchat, Inc.

- Issue
  - False or misleading regarding disappearance of snapchats

In the Matter of Snapchat, Inc.

- “Snapchat provides a mobile application that allows consumers to send and receive photo and video messages known as ‘snaps.’ Before sending a snap, the application requires the sender to designate a period of time that the recipient will be allowed to view the snap. Snapchat markets the application as an ‘ephemeral’ messaging application, having claimed that once the timer expires, the snap ‘disappears forever.’”

In the Matter of Snapchat, Inc.

- Are videos really gone?
  - Use of a computer and simple tools to locate and save the video
  - 3rd party applications to download and save videos and pics
  - Easy to circumvent screenshot notification detection mechanism
In the Matter of Snapchat, Inc.

- "Snapchat has represented, expressly or by implication, that when sending a message through its application, the message will disappear forever after the user-set time period expires. [True] In truth and in fact ... when sending a message through its application, the message may not disappear forever after the user-set time period expires. Therefore, the representation ... is false or misleading."

In the Matter of Snapchat, Inc.

- Result
  - 20 years of monitoring

FTC Consent Decrees

- Elements include "(1) prohibition on the activities in violation of the FTC Act; (2) steps to remediate the problematic activities, such as software patches or notice to consumers; (3) deletion of wrongfully-obtained consumer data; (4) modifications to privacy policies; (5) establishment of a comprehensive privacy program, including risk assessment, appointment of a person to coordinate the program, and employee training, among other things; (6) biennial assessment reports by independent auditors; (7) recordkeeping to facilitate FTC enforcement of the order; (8) obligation to alert the FTC of any material changes in the company that might affect compliance obligations (such as mergers or bankruptcy filings)."
Types of Section 5 Privacy and Security Violations

• “Deception” prong
  – “FTC brings cases for broken promises of privacy, general deception, insufficient notice, and unreasonable data security practices.”

Types of Section 5 Privacy and Security Violations

• “Unfairness” prong
  – “[T]he FTC brings cases for retroactive changes to privacy policies, deceitful data collection, improper use of data, unfair design or unfair default settings, and unfair data security practices.”

Retroactive Changes to Privacy Policies

• “Gateway altered its privacy policy to allow the renting of personal information to third parties without informing customers and obtaining their explicit consent. The FTC filed a complaint alleging that this practice was an unfair and deceptive act. According to the FTC, Gateway’s retroactive application of a materially changed privacy policy to information that it had previously collected constituted an unfair practice. The FTC also charged that Gateway’s failure to inform consumers of its changes to its privacy policies, despite its promises to do so, constituted a deceptive practice.”
In the Matter of Facebook, Inc.

• Issue
  – Availability of certain posted information to unknown people

—

In the Matter of Facebook, Inc.

• “Facebook has designed its Platform such that Platform Applications can access user profile information in two main instances. First, Platform Applications that a user authorizes can access the user’s profile information. Second, if a user’s ‘Friend’ authorizes a Platform Application, that application can access certain [parts] of the user’s profile information, even if the user has not authorized that Application. For example, if a user authorizes a Platform Application that provides reminders about Friends’ birthdays, that application could access, among other things, the birthdays of the user’s Friends, even if these Friends never authorized the application.”

108

In the Matter of Facebook, Inc.

• “[Nothing on Facebook] disclosed that a user’s choice to restrict profile information to ‘only Friends’ or ‘Friends of Friends’ would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to ‘only Friends’ or ‘Friends of Friends’ accessible to any Platform Applications that the user’s Friends have used (hereinafter ‘Friends’ Apps’). Information shared with such Friends’ Apps has included, among other things, a user’s birthday, hometown, activities, interests, status updates, marital status, education (e.g., schools attended), place of employment, photos, and videos.”

109
In the Matter of Facebook, Inc.

• “[O]n approximately November 19, 2009, Facebook changed its privacy policy to designate certain user information as ‘publicly available’ (‘PAI’). On approximately December 8, 2009, Facebook began implementing the changes referenced in its new policy (‘the December Privacy Changes’) to make public in new ways certain information that users previously had provided.”

In the Matter of Facebook, Inc.

• “Before December 8, 2009, users could, and did, use their Profile Privacy Settings to limit access to their Friend List. Following the December Privacy Changes, Facebook users could no longer restrict access to their Friend List through their Profile Privacy Settings, and all prior user choices to do so were overridden, making a user’s Friend List accessible to other users. Although Facebook reinstated these settings shortly thereafter, they were not restored to the Profile Privacy Settings and instead were effectively hidden.”

In the Matter of Facebook, Inc.

• “Facebook failed to disclose, or failed to disclose adequately, that, following the December Privacy Changes, users could no longer restrict access to their Name, Profile Picture, Gender, Friend List, Pages, or Networks by using privacy settings previously available to them. Facebook also failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user’s Name, Profile Picture, Gender, Friend List, Pages, or Networks. These facts would be material to consumers. Therefore, Facebook’s failure to adequately disclose these facts, in light of the representation made, constitutes a deceptive act or practice.”
In the Matter of Facebook, Inc.

- “[B]y designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers. This practice constitutes an unfair act or practice.”

In the Matter of Facebook, Inc.

- “Facebook has shared information about users with Platform Advertisers by identifying to them the users who clicked on their ads and to whom those ads were targeted… Facebook has represented, expressly or by implication, that Facebook does not provide advertisers with information about its users. … Facebook has provided advertisers with information about its users. Therefore, the representation set forth … constitutes a false or misleading representation.”

In the Matter of Sears Holdings Management Corp.

- Issue
  - Did SHMC violate Section 5(a) of the Federal Trade Commission Act?
  - My SHC Community related app developed by a third party
In the Matter of Sears Holdings Management Corp.

- "The Application, when installed, runs in the background at all times on consumers’ computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of respondent. Information collected and transmitted includes: web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services."

In the Matter of Sears Holdings Management Corp.

- How was information communicated to users?
  - Pop up with information
  - Follow up email
  - Registration page with "Privacy Statement and User License Agreement"

In the Matter of Sears Holdings Management Corp.

- "When installed, the Application functioned and transmitted information substantially as described in the PSULA. The Application, when installed, would run in the background at all times on consumers’ computers. Although the Application would be listed (as ‘mySHC Community’) in the ‘All Programs’ menu and ‘Add/Remove’ utilities of those computers, and the Application’s executable file name (‘srhc.exe’) would be listed as a running process in Windows Task Manager, the Application would display to users of those computers no visible indication, such as a desktop or system tray icon, that it was running."
In the Matter of Sears Holdings Management Corp.

• "The Application transmitted, in real time, tracked information to servers maintained on behalf of respondent. The tracked information included not only information about websites consumers visited and links that they clicked, but also the text of secure pages, such as online banking statements, video rental transactions, library borrowing histories, online drug prescription records, and select header fields that could show the sender, recipient, subject, and size of web-based email messages."

In the Matter of Sears Holdings Management Corp.

• “[R]espondent has represented, expressly or by implication, that the Application would track consumers’ ‘online browsing’ Respondent failed to disclose adequately that the software application, when installed, would monitor nearly all of the Internet behavior that occurs on consumers’ computers to respondent’s remote computer servers. These facts would be material to consumers in deciding to install the software. Respondent’s failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice.”

In the Matter of Sears Holdings Management Corp.

• “Respondent’s failure to disclose these [relevant] facts, in light of the representations made, was, and is, a deceptive practice.”
COPPA

- Children’s Online Privacy Protection Act of 1998 (COPPA)
- Children’s Online Privacy Protection Rule of 2013

COPPA Violations

- §6502(a) Acts prohibited (1) In general
- It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b) of this section.

Children under COPPA

- A child under COPPA is a person under the age of 13
  - COPPA is not applicable to children over the age of 13
Do You Collect Personal Information from a Child?

- Website is directed to a Child and you collect PI from them (or let others collect PI from them)
- Website is directed to a general audience, but you have actual knowledge you collect PI from Children
- Ad network or plugin and you have actual knowledge you collect PI from Children

Personal Information

- What PI fall under COPPA?
  - Full name
  - Home or physical address
  - Online contact information including email address
  - Screen or user name
  - Telephone number
  - Social security number
  - Persistent identifiers including cookies and IP address
  - Photos and videos containing a child’s image or voice

Must Post a COPPA compliant Privacy Policy

- Link privacy policy on homepage
- Include
  - List of all operators collecting PI
  - Description of the PI collected and how it's used
  - Description of parental rights
**Parental Involvement**

- Notify parents directly before collecting PI from their kids
- Obtain parental verifiable consent before collecting PI from their kids
- Honor parents ongoing rights by
  - Allow parents to review collected PI
  - Provide a manner to revoke consent
  - Allow for a requested deletion of child’s PI

---

**Program Completed**

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