Core Curriculum Supplement

Academic Unit / Office NSM/Computer Science **Catalog Year of Implementation** 2019-2020

Course (Prefix / Number) COSC / 4311 **Course Title** Computer Scientists and Society

Core Proposal Request

☒ Add to Core Curriculum ☐ Revise course already in Core Curriculum

	Current Core Categorization (New additions: select N/A for this column)	**Proposed Categorization for Upcoming Core**
Foundational Component Area (required)	N/A (Not currently a Core course)	Social and Behavioral Sciences (80)
Component Area Option (optional)	N/A (No Component Area Option)	Writing in the Disciplines (81)
Category Listing: Single or Double?	N/A (Not currently a Core course)	List under the Component Area Option ONLY.

Core Proposal Rationale - Please provide a rationale for including, or continuing to include, this course in the UH Core Curriculum:

This course meets the objectives of a writing in the discipline course. At this point, there is no course that addresses writing in the discipline of computer science.It is designed to teach students:

1. Legal issues that have direct bearing on their profession as computer scientists, such as intellectual property.
2. Writing technical reports on issues that are at the intersection of computer science and the law.
3. Making presentations on specific scenarios that lie at the intersection of computer science and the law.

Core Objectives *(see THECB Core objectives)*

☒ Critical Thinking ☐ Teamwork

☒ Communication ☒ Social Responsibility

☒ Empirical & Quantitative Skills ☐ Personal Responsibility

Please explain how the Core Objectives selected above will be met:

The course objective is to introduce and to discuss issues of professional responsibility and ethics related to the use of computer technology in complex modern working environments. Emphasis on specific cases, on group discussion, and on oral presentations and written reports by students. The basis for the cases is a set of articles taken from the Communications of the ACM (Association for Computing Machinery) such as (a full list is attached):

1. Copyright for Software: Changes in the Past 20 Years in Laws and Public Perception
2. Software Patents since 1970 in the US and the EU: Objectives, Procedures, Obstacles.
3. Legal and Technical Ramifications of "Hacking"
4. Legal Liability Issues Related to Faulty Software
5. Corporate Responsibility Related to Data and Information: Contrast US and EU Approaches
6. The Controversies Surrounding Key Escrow, Including Technical Aspects and Legal Ramifications

7. Ethics and Legal Issues Related to the Distribution of Undesirable or Illicit Material via the Internet

---

When submitting this proposal form, please remember to attach a syllabus, learning objectives, and/or sample lesson(s).

Why Should COSC 4311 Be a Writing in the Discipline Course?

Ernst L. Leiss
16 April 2018

This course has been taught, in various incarnations, for over twelve years. It is designed to teach students:
1. Legal issues that have direct bearing on their profession as computer scientists, such as intellectual property.
2. Writing technical reports on issues that are at the intersection of computer science and the law.
3. Making presentations on specific scenarios that lie at the intersection of computer science and the law.

Each student must write an extensive report, 12-18 pages, in a format that is appropriate for a technical report. Each student must write independently on a uniquely assigned topic, referred to as an "abstract notion" (that is, no two students write about the same topic). In addition, each student must write two papers, 4-8 pages each, about a specific scenario that presents a legal and ethical dilemma directly related to the profession.

Each student must present his or her work on the assigned abstract notion (20 min, with PowerPoint slides); each student must present his or her work on one of the two selected scenarios (15 min, with PowerPoint slides), including determination about legality and ethicality of each action of each actor in the scenario.

The abstract notions are selected by each student from a master list of topics (attached) which typically varies from semester to semester (only a subset of the master list is offered each semester). The scenarios are selected from the two Self-Assessment Procedures IX and XXII (CACM Vol. 25, No. 3 and Vol. 33, No. 11). All assessments and determinations must be based on the legal situation at the time of writing.

Students are instructed how to write technical reports, how to research the types of topics discussed in the course, and how to make presentations. All presentations and all reports are graded independently for format and for content; thus, two grades are generated, one which reflects an assessment of the way in which the report or presentation are given, the other an assessment of the content.

The course has been taught by Ernst Leiss continually since at least 2005. A lecturer has taught this course regularly, typically once a year, for several years now. Jaspal Subhlok should also be qualified to teach this course.

It is my definite opinion that this course more than meets the objectives of a writing in the discipline course. At this point, there is no course that addresses writing in the discipline of computer science. I strongly believe that the department should provide a course on technical writing that deals with computer science, rather than some other discipline.

COSC 4311 Computer Scientists and the Society

Section 13298

Instructor: Ernst L. Leiss
Textbook: A Gift of Fire, Sara Baase, Prentice Hall (ISBN 9780132492676)
Time: Mo, We, 2:30- 4 pm
Place: AH 201

Prerequisites: COSC 3480, and COSC 4351 or 4330; and successful completion of all of the university core curriculum. **Exceptions will only be made if this is your last semester**. **This course should be taken in the student's LAST semester**.

Catalogue Description: Introduction and discussion of issues of professional responsibility and ethics related to the use of computer technology in complex modern working environments. Emphasis on specific cases, on group discussion, and on oral presentations and written reports by students.

GRADES, HOMEWORK, ETC.

1. All assignments are due at the hour and on the day as specified. There will be **no late assignments**. The assignments are writing exercises as well as content-oriented. Your grade will depend on both aspects.
2. There will be one abstract notion paper, due on **We, March 7, 2018**; two papers covering two scenarios from the Self-Assessment Procedures, both due on **We, April 18, 2018,** a 20-min presentation of the abstract notion (AN) paper (**on Saturday, March 3, from 10 am until 6 pm**), and a 17-min presentation of one of the selected two scenarios (**on Saturday, April 14, from 10 am until 4 pm**). In addition, there will be a short examination, probably on **Monday, April 23**, over the material covered in class and your talks.
3. The final grade will be formed as follows:

   30% AN Paper **15% AN Presentation** **15% Each Scenario Paper**
   10% Scenario Presentation **15% Examination**
4. Requests for grade adjustments will be considered only during the 3 working day period after the graded material has been returned to the class. Later requests will not be considered under any circumstance.
5. Students requesting accommodation under the Americans with Disabilities Act (ADA) must notify the instructor, in writing if possible, by Wednesday, June 7, 2017, of their request.
6. Office hours: **Tu, Th: 12 – 12:30 pm**. Note: **Content** questions will only be answered in class.
7. **You must attend the first day of class.** Failure to attend the first day of class may get you dropped from this course.

The course is taught based on cases rather than as a traditional ethics course. It is a cap stone course relating the technical computer science knowledge to questions of ethics and professionally responsible behavior as computer scientists. The basis for the cases is a set of articles taken from the Communications of the ACM (Association for Computing Machinery), including in particular two self-assessment procedures on these issues. While many technical topics lend themselves naturally to binary conclusions (works – does not work; true – false; etc.), students must appreciate that the issues central to this course do not. To this end, class discussions, including oral presentations, as well as written reports, are emphasized.

There will be several lectures by the instructor, covering among others: Introduction Motivation, Overview [GF]; ACM Code of Ethics, Discussion [CACM 5/92, 2/93; GF]; Legal Issues and Procedures [CACM 5/85]; Liability [CACM 1/93] and Unreliable Software [GF]; Crime/Computer as Tool [GF]; Copying; Privacy [GF]; Encryption; Background [Leiss 82] and Controversies [CACM 7/92]; Viruses and Worms [GF; Leiss 90]

CACM: Communications of the ACM **Leiss 82: Principles of Data Security, Plenum 1982.**
GF: Gift of Fire (textbook) **Leiss 90: Software Under Siege: Viruses and Worms, Elsevier, 1990.**

You must write three papers and make two oral presentations. All papers must include references to a significant body of literature that you have researched. All papers must have normal margins, be double-spaced, use font of pitch 10-12, and must be handed in as hardcopy. One paper deals with one of the Abstract Notions listed below; this paper should be about 12-18 pages long. The other two papers deal with two **substantially unrelated** scenarios you must select from the two Self-Assessment Procedures; each of these two papers should be about 4-6 pages long. The first oral presentation covers the abstract notion you chose/were assigned. The second oral presentation covers one of the two selected scenarios.

On **Monday, Jan. 29**, each student must submit in writing (**hardcopy**) in class at **2:30 pm sharp the numbers of THREE Abstract notions** that the student is prepared to present and write about. When turning in the Abstract Notion paper, each student must also indicate which two scenarios were selected and which one will be presented.

Master List

Topics for Abstract Notion; note you may **not** modify the title and must treat comprehensively the **entire** topic described by the title:

1. **Copyright for Software: Changes in the Past 20 Years in Laws and Public Perception**
2. **Software Patents since 1970 in the US and the EU: Objectives, Procedures, Obstacles.**
3. **Legal and Technical Ramifications of "Hacking"**
4. **Legal Liability Issues Related to Faulty Software**
5. **Corporate Responsibility Related to Data and Information: Contrast US and EU Approaches**
6. **The Controversies Surrounding Key Escrow, Including Technical Aspects and Legal Ramifications**
7. **Ethics and Legal Issues Related to the Distribution of Undesirable or Illicit Material via the Internet**
8. **Issues Related to Intellectual Property Rights: Compare US and EU Approaches**
9. **Cryptographic Techniques as Munitions: US Export Controls and EU Approaches**
10. **The Notion of Privacy: Compare US and EU Approaches**
11. **Carnivore, Echelon, etc.: Discuss Technical Aspects as well as US and EU Privacy Concerns**
12. **Napster/Gnutella/BitTorrent etc.: Discuss Legal and Technical Aspects**
13. **The Motion Picture Association of America and DVD Encryption: Discuss Technical and Legal Aspects**
14. **E-signatures and Digital Signatures: Discuss Technical and Legal Foundations, both in the US and the EU**
15. **Should Programmers Be Required to Be Certified as Professional Engineers? Discuss Historic Developments and Outlook**
16. **Spam: Issues and Methods for Reducing/Eliminating It**
17. **The Tension between Standards and Patent Protection**
18. **DRM: Discuss Technical and Legal Aspects**
19. **E-cash and Related Proposals: Issues, Limitations, Legal and Technical Aspects**
20. **Ownership Issues Related to IP Posted on Social Network Sites, such as Facebook**
21. **Reverse Engineering versus the Digital Millennium Copyright Act and Related US and EU Legislation: Discuss Technical and Legal Aspects**
22. **E-voting: Controversies, Legal Challenges, and Technical Difficulties and Solutions**
23. **Should Artists Be Allowed to Control the Use, Display, and Disposal of their Artistic Creations after their Sale? Discuss Legal and Ethical Aspects**
24. **Compulsory Licensing: Legal and Ethical Arguments for and against**
25. **EBay versus Bidder's Edge: Discuss Technical, Legal, and Ethical Aspects**
26. **Net Neutrality: Discuss Technical, Legal and Policy Issues; Review the History of Legislative Efforts**
27. **Fair Use: Discuss Legal Aspects and Challenges, Including Technological Inhibitors and Mash-ups**
28. **Spectrum Allocation and the LightSquared Affair: Discuss Technical, Political and Ethical Aspects**
29. **Who Owns, Who Operates/Manages the Internet? Discuss Business Model; Funding of Infrastructure, Improvements, Management, and Operations (Past, Present, and Future); Politics, including Recent Efforts by the UN; and Ethical Implications thereof**
30. **Compelling an Accused to Divulge the Password for an Encrypted Object that Might Incriminate the Divulger: Discuss Legal Context, Precedents, Politics, and Ethics**
31. **Employers Requiring Applicants, Colleges Requiring Scholarship Recipients to Allow Access to their Social Media Accounts. Discuss Legal Context, Public Reaction, Ethicality, and Implications for the Monitoring Agent**
32. **The Tor Project and other Anonymizing Tools: Technology, Ethics, and Legality**
33. **US Surveillance of Citizens without Court Order: History, Laws, Processes, and Ethics over the Past 20 Years**
34. **Secret justice: From sealing court orders to National Security Letters to FISA to No-Fly lists – The role of secrecy in administering justice in the US and the EU**
35. **(Ab)Using software to circumvent regulations – VW's emission control software, ERCoT's charging program, Uber's Greyball, and similar code**
36. **The legality and ethics of collecting air traveler information and its use to deny access to transportation – US and EU**
37. **The controversies that surround unlocking cell phones: Legal, technical, commercial, and ethical aspects**

F: C
C: A-

P

[redacted]

Issues Related to Intellectual Property right: Compare US and EU approaches.

Computer Scientists and the Society

[redacted]

Abstraction

European Union laws on intellectual property are more in support of the creator than the public, this conclusion is derived from the difference between the United States and European Union laws on intellectual property. In the united states, the laws are more forgiving on the public and this is illustrated in the copyright, trademark, patent laws that as pass in the United States. United states laws are in strong support of innovation and competition. My Approach to this paper was strictly based on comparing the differences between European union and United States laws on intellectual property and with a brief introduction of what is the official definition of intellectual property between both countries. I Mentioned the types of intellectual properties which are; trademark, trade secret, plant varieties, copyright and patents and pivot on trademark, patent and copyright. In copyright, explained moral rights and fair use. In trademark, explained dilution and renewal and in patents, I elaborate on first to file and first to invent, grace period, best mode requirement and opposition after granted.

Extremely sloppily written — did you proof-read this at all??

Table of content

Introduction:

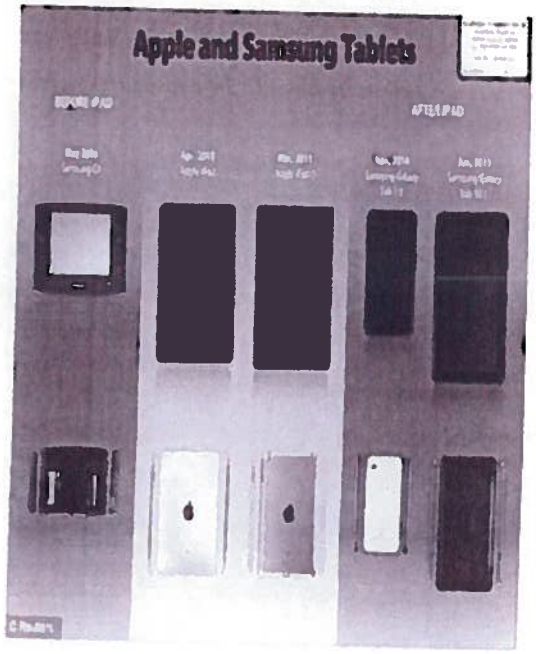
Most people believe that intellectual property laws are outdated, overrated and pretty much irrelevant to the modern day. Some people don't think about it at all, but it's a topic that impact our everyday life. Many people knowing or unknowing violate the intellectual property laws that if enforced properly, they could be sued for millions of dollars. Most of the people that argue against intellectual property laws say that "information just wants to be free". The quote "information just wants to be free" is taken from Stewart Brand. Stewart brand gave a speech to the group of computer science in 1994 and he also stated that "in the other hand that information wants to be expensive because it's so valuable. The right information in the right hands can change lives" and "in the other hand that information wants to be free, because of getting it out is getting lower and lower and all the time. So, you have this two fighting against each other." I totally agree with this quote because as the technology advances with faster internet and cheaper computers over time we move further into the information age. The worth of information become extremely valuable but at the same time sharing becomes extremely easy which make is difficult track and almost impossible to control and distribute. This brings the argument what is the difference between the laws that govern intellectual property in European Union and united states, and how does it affect the life of the creator and the public.

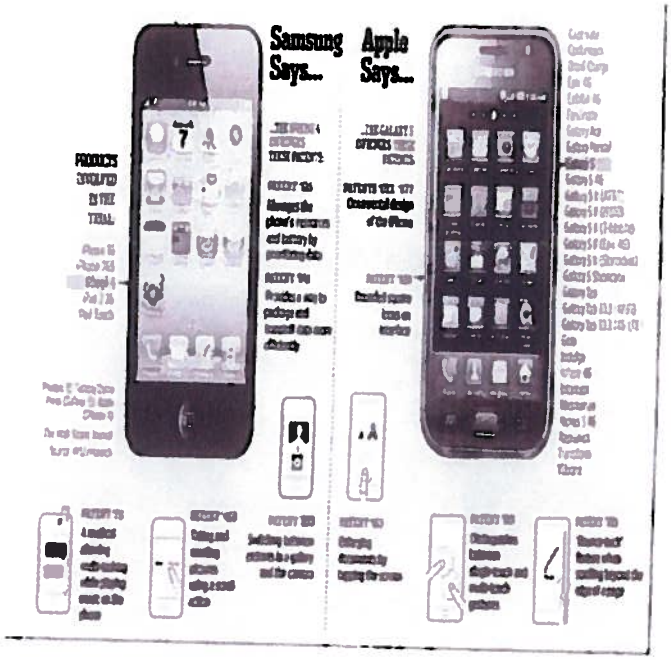
In the united states, "article I, section 8 of the United states constitution gives congress express authority to grant and inventors exclusive rights to their creations. Section 8 also gives Congress the power to regulate interstate and foreign commerce, providing further support for its right to legislate in this area. Intellectual property laws passed by Congress are administered by two government agencies, the U.S. Patent and Trademark Office, and the U.S. Copyright Office" [1] USPTO. As technology advance different amendments has been conducted on the original constitution to meet with the times. Scroll of the piano roll was identify on the constitution in the 1909 copyright act and it covered all intellectual work on the scroll. later, In 1976, the photocopier was identify on the constitution and it covered all the works that photocopied and distribution. Finally, in 1998 internet was cover in the digital millennium copyright act. While in European union, "intellectual property rights as a result 28 European countries with the goal increasingly knowledge-based economies, the protection of intellectual property which is important for promoting innovation and creativity, developing employment, and improving competitiveness"[2] EPO. The European Commission works to harmonies laws relating to industrial property rights in EU countries to avoid barriers to trade and to create efficient EU-wide systems for the protection of such rights. It aims to fights against piracy and counterfeiting and to help businesses, especially small businesses with access and use intellectual property rights more effectively that said when compare with other developing countries for example the united states, we can see that the European union aim is to support business with the intellectual property.

Run-on sentences

I give you the 10-word rule! Use it!!

History and famous cases: Samson vs Apple





Samsung and apple case is a long-standing dispute between two major mobile phone manufactural company. The supreme court case was focus on whether Samsung infringement on the iPhone patent and how Samsung should be punished. The question was that if Samsung should turn in every single account that they have made from product or they should pay based on the product value to the product. Samsung was asked by the supreme court to pay apple the total about of money made from selling galaxy device and Samsung appealed the case by saying that the reason that people were paying the device wasn't because of the rounded edges or a

button at the particular location and they should pay base on the product. But the supreme court ruled in favor of apple and Samsung was order to pay 1 billion dollars to apple. Samsung decide to pay one million dollars to apple in nickels. The money was delivered to apple in 30 trucks.

Types of Intellectual Property and meaning

In this paper, we will briefly go through all the types of intellectual property and will focus on three major types of intellectual property; patent, copyright, and trademark. They are six types of intellectual property rights called patents, copyright, Trademark, trade secret, trade dress and plant varieties etc.

Trade secret: Trade secret according to Wikipedia is defined as any formula, practice, process design, instrument or pattern which is not generally known that gives a business an economic advantage. For an example, McDonald is believed to have a special sauce that makes its fries to

taste good. This sauce is protected under trade secret right and who ever reveal the trade secret is punished by the law. Trade secret has no limitation in the number of renewal.

Trade dress: Trade dress is a legal term of art that generally refers to characteristics of the visual and aesthetic appearance of a product of packaging. If you remove the trade mark and the sentences/words from the packages the rest of the design and aesthetic can be protected on the trade dress law. In the case of organic popcorn and simply nature popcorn, the two bowl have different color and they all have distinguishing text fonts. The top of the packages has a very distinguishing design and all this difference can be file under trade dress.

Plant Varieties: Plant variety rights (PVRs) are presently available for "varieties of any kind of plant other than algae and bacteria. The word "variety" is used not in the sense of a "botanical variety", but rather as being synonymous with "cultivar" or "cultivated variety"."[3] Plant Variety Rights give you the additional exclusive commercial right to propagate the variety for the commercial production of fruit, flowers or other products of the variety. Plant right control over commercialization of a variety.

Patents

In the United States, "the patent for an invention is the grant of a property right to the inventor, issued by the United States Patent and Trademark Office. Generally, the term of a new patent is 20 years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. U.S. patent grants are effective only within the United States, U.S. territories, and U.S. possessions"[1] USPTO. Under certain circumstances, patent term extensions or adjustments may be available while in the European union, "A patent is a legal title that can be granted for any invention having a technical character if it is new, involves an 'inventive step', and is susceptible to industrial application. A patent can cover how things work, what they do, what they are made of and how they are made. Anybody can apply for a patent for an invention"[2] EPO. United states and European union both have a similar definition of patent but they are still differences on how the laws can implemented. As I previously mentioned United States intellectual laws flavor the user of an invention rather the creator. I will use the difference in the patent laws to outline my point. Until 2013, the united states operated on first to invent, which means if an inventor can proof with an extensive document that he/she invented the invention first he/she have the right over

the invention. While in the European union, they have always operated on first to file which means who ever file for the invention has the right over the invention. In the united states the grace period to file for a patent right once the patent has been exposed to the public is one year compare to European union which once the patent has been exposed to the public the inventor can't file for a patent right for the invention. This can be a barrier for inventors testing their invention in the market but at the same time a positive. becoming the first to file a year later after the patent has been release can cause a lot of conflict to the inventor that believe they came up with the invention first. Finally, the united stated the inventor is required by law to add the best mode requirement to avoid the investor adding a little more portion and extending the patent term with another 20 years while in the European union the inventor best mode for the invention is not required. This further proof that united states laws compare to European laws are stricter on inventor than the users/public.

Copyright

in the United States, "Copyright is a form of protection provided to the authors of "original works of authorship" including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished. The 1976 Copyright Act generally gives the owner of copyright the exclusive

right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phono records of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly"[1] USPTO. ~~While~~ In European Union, "The EU copyright legislation is a set of ten directives, which harmonies essential rights of authors and of performers, producers and broadcasters. By setting harmonized standards, the EU law reduces national discrepancies, ensures the level of protection required to foster creativity and investment in creativity, promotes cultural diversity and ensures better access for consumers and business to digital content and services across Europe"[2]. United states and European union both have a similar definition of copyright laws but with subtle differences, in the United States copyright is used to protect authors while in European union, copyright is used to protect author, performers, producers and broadcasters. As I previously mentioned, United intellectual laws flavor the user of an invention rather the creator. I will use the difference in the copyright to outline my point again. The European union definition of copyright is extensive of the creator while in the united states, only author is primary protected. They are two most significant difference between European union and united states laws on copy and they are moral rights and fair use. In the united states when it comes to moral rights, the author of a piece of work still has control of his/her work if do it been sold and this rights can't be waiver or transfers. This means that when a buyer buys a book, he has control to read, destroy, sell the book but he don't have the power to reproduce more copies or modify the book. In the European union, this right can be waive or transfer to the buyer and he can make copies and sell or modify it. When it comes to fair use, the united states fair use laws are very broad and they are many factor that can qualify a piece of work a fair use. One of the factor is purpose of the copied

work. Depending on the purpose of the work, it could be considered fair use if it's for education or training purposes. Another effect on the market of the original work is not consider fair use if as a result of the copying the work, it reduces the worth of the work or make it unsellable. In the European Union, it's very restricted and tightly defined with certain exclusions and limitation to copyright.

Trade Mark

In United stated, "A trademark is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others. A service mark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. The terms "trademark" and "mark" are commonly used to refer to both trademarks and service marks"[1] USPTO while in Europe, "A trade mark is a sign which distinguishes the goods and services of one company from those of another. As indicators of business origin, trademarks can be words, logos, devices or other

distinctive features, or a combination of these. They can also be referred to as 'brands'."[2] United states and European union both have a similar definition of trade are similar but with subtle differences, in the united states trademark is used to distinguishes the source of the service while in European union, trademark is used to distinguishes the goods. As I previously mentioned, United States intellectual laws favor the user of an invention rather the creator. I will use the differences in the trade laws to outline my point again. In the united states and European union, trademarks must be renewed every five years but the united states added a little more requirement. If an inventor that possess the trademark doesn't use the trademark for 5 year in the united states, he/she can lose the right to renewal the trademark but this doesn't apply in the European Union. In European union, an inventor can hoard the trademark. Dilution is when a trademark's public image is damage by another company that may not be in directly competition. This occurs when a company decides to open a gentlemen's club called MccDonald with a double c. If the public image of the MccDonald is not what McDonald wants to be associated with, McDonald can sue MccDonald for diluting the trademark or brand. In the United States and European union, they are many criterias that may grant McDonalds the right to sue. In the united states the mark must be used in the United States, it must be famous mark and widely recognized by the general consuming public. While in the European Union, the trademark doesn't need to be famous but just known by the significant part of the public.

Conclusion

My Approach to this paper was from a very general perspective, I didn't know what I ~~will~~ discover during my research. After reading numerous papers and websites, I have come to personal conclusion that the united states laws on intellectual property ~~is~~ built to support innovation and to stimulate creativity. United states is gives inventors a years after patents ~~expose~~ and it allows fair use which is good. That bring me to the final conclusion that intellectual property laws in the united states support the citizen and breaks the barriers of expression and being inspired.

Reference

1. Resources, Inventor. "General information concerning patents." *United States Patent and Trademark Office - An Agency of the Department of Commerce*, www.uspto.gov/patents-getting-started/general-information-concerning-patents.
2. "Patent protection in the EU - Growth - European Commission." *Growth*, ec.europa.eu/growth/industry/intellectual-property/patents_en.
3. "The EU copyright legislation." *Digital Single Market*, European Union Commission,
    a. ec.europa.eu/digital-single-market/en/eu-copyright-legislation.
4. "What is a Trade Secret?" *What is a Trade Secret?*, WIPO, www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm.
5. Engelfriet, Arnoud. "Differences between US and European patents." *Ius mentis*, 1 Oct. 2005, www.iusmentis.com/patents/uspto-epodiff/.
6. Stim, Richard. "What Is Fair Use?" *Stanford Copyright and Fair Use Center*, 11 Apr. 2017, fairuse.stanford.edu/overview/fair-use/what-is-fair-use/.
7. Satterthwaite, Janet F. "US and European trademark practice compared." *Lexology*, 5 Aug. 2011, www.lexology.com/library/detail.aspx?g=42d3b205-b225-4703-af7d-13efeb100571.

P

F: C+

C: A-

This is awful

A CAMPAIGN TO THWART ILLEGAL COPYING

Digital Rights Management has become the bearer of continuing the war on piracy. A creation to update past legislation and its enforcement of media content. DRM is now accompanied with almost every digital good. Each one with a mission to prevent unauthorized actions deemed undesired by copyright holders. From its initial stages to present day, the provision has struggled against opposition. Technical bypasses and legal oversights have shaped DRM's variability. Early cryptic and ludicrous implementations have steered its advancement to subtleness. However, with technological improvements comes an ever-growing community that overcomes its lawful enforcement. No matter the consequences, piracy is still vastly present among this community. An overwhelming force that continues to prove DRM is far from being a perfect anti-circumvention provision. Industries of digital media content can decide whether to enact such methods to protect their goods. All the while considering the economic opportunities and setbacks. At the same time, avoiding past and unprecedented legal disturbances among the public.

A provision struggles??

More than half of what you wrote are not proper sentences!

[redacted]

March 3rd, 2018

A Campaign to Thwart Illegal Copying

[redacted]
University of Houston
clliothenriq@gmail.com

March 3rd, 2018

Table of Contents:

goal

"Flow of consciousness" is a lousy way to write a report. Your reports must consist of sentences, written in standard English. If something is not parsable, it is wrong!

1. Introduction to Digital Rights Management

Over the last twenty years, an explosion of digital media goods has become more available and affordable. An avenue for media industries and copyright holders has opened to extend their markets in enormous fashion. With these goods comes provisions to ensure legitimate usage and consumerism. Infamously known as DRM, Digital Rights Management is an "access-control technology used by manufacturers, publishers, and copyright holders to limit the usage of digital devices or information [1]." There are numerous technologies that are employed as DRM. These technologies control how authorized digital content and purchases are used. They limit the intended use of products to keep it legitimate. In other words, they also prevent unauthorized use of said products. Activities such as mass-producing copies or bypassing security mechanisms would be examples of unauthorized uses [2].

Background History

Before the creation of DRM, copyright holders needed means to inform consumers of copyright infringement. One such method was the FBI Anti-Piracy Seal that was shown to discourage content copying and distribution. An example of the seal is shown below in Figure (1). This effort took hold many years before DRM. Produced was the Copyright Act of 1976 which established a foundation of copyright laws in the advancement of technology [3]. However, a warning was not enough to deter unauthorized distributors from illegally copying movies. With rising availability of the Internet in the 90s, it became more difficult to prevent anti-piracy activities.

(1)

2. Emplaced Legislation

Like most legislation, copyright laws began as an interest to major media companies. Lobbying their way to Washington, these industries would encourage representatives of the government to enact such a law to protect their goods. In exchange, they would be financially or politically supported for their service.

The Digital Millennium Copyright Act

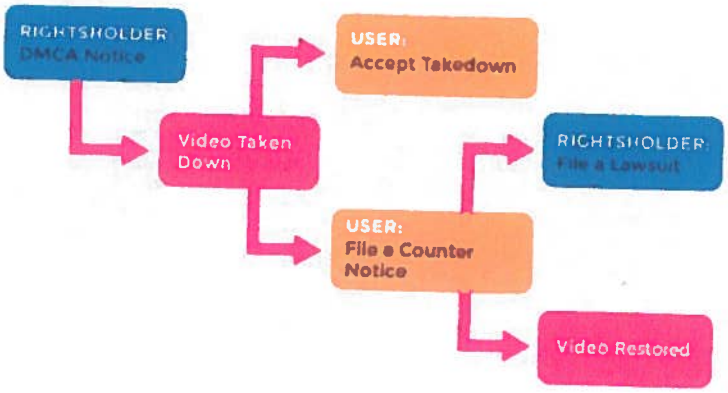
In October 1998, the DMCA was passed under the Clinton administration. Its purpose was to modernize U.S. copyright laws for the digital age. The DMCA criminalizes acts that bypass access-control technology. Whether it infringed on copyright laws did not matter [4]. Many provisions were enacted under the DMCA, including the establishment of DRM. It allowed for copyright holders to set these technology restraints in products to prevent them from being reproduced.

Provisions

The act also gave online and internet service providers havens from liability [4]. Say if a person were discovered downloading content in any fashion that wasn't legitimate, they would receive a DMCA notice from their ISP. Figure (2) shows a basic model of the notice process. A way of notifying a person to cease any activity that constituted copyright violation or face legal

consequences. Many people have already experienced the latter, such as Joel Tenenbaum, who was sentenced to pay $675,000 for downloading and sharing 30 songs online [5]. A huge price to pay for such a small act. However, in the eyes of the law, this act is considered as stealing. As well as stealing from major record companies that hold the copyright, the value of these products becomes amplified. It makes a person reconsider their decisions with these kinds of penalties.

(2)



3. Mission of DRM

With the DMCA came the many forms of DRM. It would be plausible to view DRM as a security to multimedia content. They are emplaced to enforce the anti-circumvention policies that were set up.

Role to Prevent

Piracy became a huge concern among media industries. Preventing copies for redistribution is the flagship mission for most DRM technologies. Its means began to stop monetary gain from those producing mass amounts of illegal copies. It slowly turned its attention to gain control and limit software mediums that enable digital content [6].

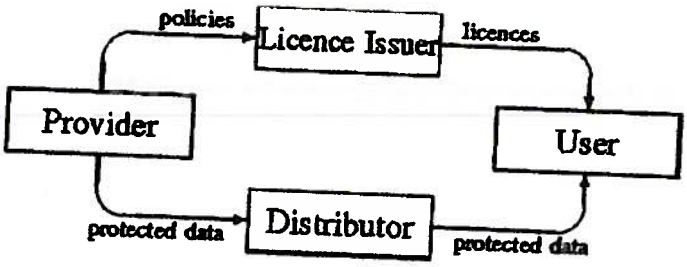
Role to Protect

The purpose to keep prevent copyright infringements also came with protection standards. Advocacy for DRM included the maintenance of artistic integrity. Legitimate distribution controls how content creations are supplied to consumers. This control also allowed industries to regulate the products' revenue stream [6]. However, this reason not completely stated to be a priority. Though it could be inferred that any loss of revenue from illegal copying is a major disturbance to businesses.

4. Implementations in the World

Mainstream products are already implemented with some technology to control the way we use it. Ranging from product authentication to encryption schemes to proprietary software. Each with a slightly different purpose though they all share a common goal. That goal is to control how content, information, and devices are used. These technologies achieve this in numerous ways and in different mediums. A simplified version of how DRM is implemented, and the parties involved in Figure (3).

(3)

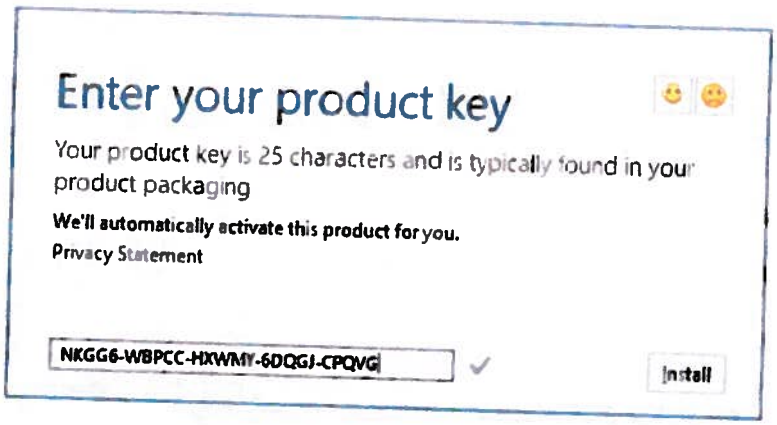


Authentication

The spectrum of digital goods includes video games, film, television, e-books, et al. Each of these types of digital content are accompanied by some form of management. Over the years, DRM has been applied to overlap one another. One of the first types of DRM were product activation

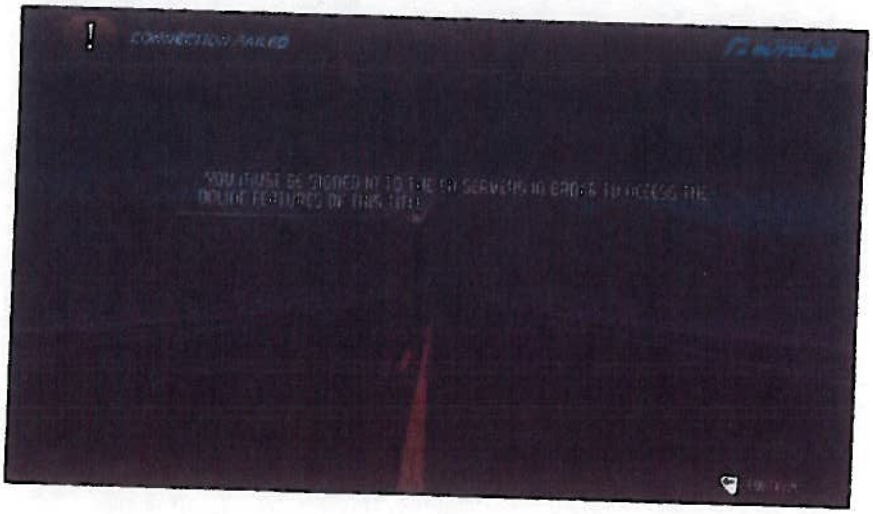
through "product keys" as shown in Figure (4). These "keys" were often serial numbers to be used as input for software as a way of authentication. It ensured that multiple copies of the same product could not be certified by the same key [7].

(4)



This method was very popular in early computer games during the 90s and early 2000s. Even limited installations were customary practice in this era. Since CD-ROMs still exist today, this method is still in practice. Especially in installations of operating systems. Though with advancement in technology, they are coupled with another form of DRM. Skip to 2018, now many digital distributors such as STEAM employ "always-on" DRM. This method usually requires constant internet connection to servers that can verify a legitimate copy [8]. Figure (5) provides a real-world example provided by Electronic Arts, Inc. So, if the internet connection drops, so does accessibility to the game.

(5)



Encryption Schemes

Another form of DRM involved are encryption schemes. In the beginning of DVD technologies, discs were sent out with encryption algorithms that utilized stream ciphers. Content Scrambling systems included ciphers that required a key for the encrypted content or information to be decrypted. However, this system used a forty-bit cipher, so it was it became susceptible to brute-force attacks [9]. A brute-force attack involves testing all possible key combinations to decrypt the cipher.

Now many media streaming services combine encryption with software such as Encrypted Media Extensions. EMEs are plug-ins that act as a middle man between content providers and DRM software. Web services encrypt their content and require a DRM software known as Content Decryption Modules to decrypt and return to the end user for playback [10]. Such software makes it difficult but not impossible for content to be copied or downloaded.

Software

Proprietary software isn't a new phenomenon in DRM technologies. An early and disastrous example would be the Extend Copy Protection. Early CD-ROMS would be accompanied by this and installed on a user's computer. A user would be prompted with an end-user license agreement. If declined, the CD would be ejected. If accepted, a software would be installed without the user's knowledge. It was shown to gain a sort of control of the computer, denying other media players or software from accessing the CD-ROM [11]. This led to public backlash and lawsuits. Luckily, this DRM technology was discontinued and served as an example of unjust DRM.

Streaming services today such as Spotify, Amazon Kindle, and Netflix use software to stream their content. It isn't as restrictive as early DRM technologies, but they are effective enough to be a deterrent for an average user from copying and/or downloading content for redistribution. Usage restrictions of digital content varies. Spotify, for example, allows unlimited downloads in their premium service but only allows access through its mobile application, software, or website. Figure (6) shows the Spotify web-based platform in which paid subscribers may access their saved music.

(6)

5. Piracy Running Amok

Going back to Joel Tenenbaum, DMCA violations are still taken seriously. Though, some unlucky few does not stop millions from bypassing DRM. A huge obstacle for copyright holders is the overabundance of available software that encourages DRM circumvention. Many web pages even include tutorials and software recommendations of said software. A simple Google search can result in a plethora of such means as shown in Figure (7). Sharing information on how to bypass DRM is not against the law itself. As a result, such information is widely available.

(7)

How to remove ebook DRM with Calibre | TechRadar
https://www.techradar.com/news/.../how-to-remove-ebook-drm-with-calibre-1291960
Jul 31, 2014 - Read your ebook purchases where and when you want. Install Calibre. Calibre is free to download, and the latest version for Windows is 1.36.0. Install the DRM remover. Calibre supports various plug-ins, and we're going to use Apprentice Alf's DRM Removal Tool for e-Books. Remove the DRM. Converting and testing.

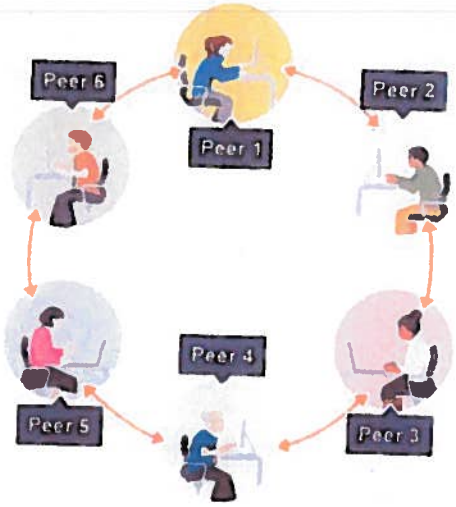
How to remove DRM from music and movies | Digital Trends
https://www.digitaltrends.com/home/.../how-to-remove-drm-from-music-and-movie-fil...
Feb 22, 2015 - Here's how to strip your music and movies of restrictions. ... Removing DRM from audio and video using Aimersoft Media Converter (Windows). ... The basic software helps you remove DRM from video and music using a Windows-based machine, thus allowing you to access your content on a variety...

Top 5 DRM Copy Protection Removal Software - Lifewire
https://www.lifewire.com › Buy › Software & Apps › Video & Audio
Jul 2, 2017 - Looking for DRM removal software? Learn about the best programs to use for removing DRM copy protection from music and video files.

Virtual Private Networks

Like old DRM technologies, the methods used today are not 100% effective. New ways of bypassing DRM are frequently being discovered. Digital content sharing has become so rampant that it seems impractical to go after every individual that circumvent content with DRM. Peer-to-peer file sharing clients such as Bit Torrent and LimeWire are widely used. Not only do these communities encourage illegal distribution, many individuals also apply Virtual Private Networks (VPNs). Each user that is part of P2P clients are often numerous and systematically support each other, Figure (8).

(8)



VPNs extend private networks to other users publically. This way users can receive and send data anonymously. This practice bypass DRM restrictions because it directly violates unlawful distribution. However, VPNs protect users by changing their geo-location, so it becomes difficult to track down users [12].

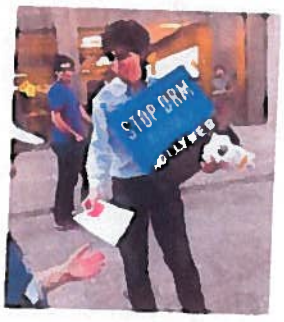
6. DRM-Free Progress

Many DRM technologies have become obsolete, and many that are utilized today are becoming easier to bypass. Nonetheless, more advanced DRM will be introduced in the future. It's up to industries to employ them. However, today publishers have begun to accept DRM-free products as business models [13]. Allowing users to be free from any restrictions and law violations. Activism is gaining support from users who support DRM-free applications (Figure 9).

Favorable Circumstances

A trade-off occurs with this venture. Publishers and content makers risk a loss of revenue by allowing unrestrictive use of the sold products. In other words, those who buy content may share and possible conduct illegal distribution without any management to prevent them from doing so. With this, it becomes more of an incentive for a customer to choose a DRM-free product over DRM-protected content because they understand they will have more freedom over their purchased good.

(9)



7. Summation

Multimedia industries made efforts to protect their digital content through copyright laws. As technology advanced, so did the easiness for copyright infringement. Digital Rights Management became a continued effort to combat piracy. A multitude of different technologies were implemented to enforce policies set by the DMCA. Though with each publication came the opposition to bypass. DRM is in a continuing war of overcoming circumvention of digital content goods.

As DRM technologies become more sophisticated, so do the tactics to crack DRM security measures. The public advocacy for DRM-free products grows ever more popular. Some companies even choose to incentivize consumers with DRM-free provisions. Only time will tell how aggressive future DRM technologies become. It will also tell if DRM-free products will be a new standard among industries.

8. Bibliography

[1] EC-Council. 2009. Investigating Network Intrusions & Cyber Crime (2nd. ed.). Computer Forensics, Vol. 4. Cengage Learning, Inc.

[2] Electronic Frontier Foundation. DRM. Retrieved March 1, 2018 from https://www.eff.org/issues/drm.

[3] Robert A. Gorman. 1977. An Overview of the Copyright Act of 1976. (Feb. 2018), 7-12.

[4] Copyright Office Summary. The Digital Millennium Copyright Act of 1998. Retrieved March 1, 2018 from https://www.copyright.gov/legislation/dmca.pdf.

[5] Javier Panzar. 2013. Large fine upheld against BU grad for illegal song downloads. Retrieved Feb. 26, 2018 from https://www.bostonglobe.com/metro/2013/06/26/court-upholds-fine-against-former-student-for-illegal-music-downloads/aXul4dPHxzv5mrnDUehaEN/story.html.

[6] Mike Masnick. 2013. True Purpose Of DRM: To Let Copyright Holders Have A Veto Right On New Technologies. Retrieved Feb. 26, 2018 from https://www.techdirt.com/articles/20130325/11132122455/true-purpose-drm-to-let-copyright-holders-have-veto-right-new-technologies.shtml.

[7] Ed Bott. 2007. A brief history of anti-piracy at Microsoft. Retrieved Feb. 28, 2018 from http://www.zdnet.com/article/a-brief-history-of-anti-piracy-at-microsoft/

[8] Wikipedia: The Free Encyclopedia. 2017. Always-on DRM. Retrieved March 2, 2018 from https://en.wikipedia.org/wiki/Always-on_DRM

[9] Gregory Kesden. G.K. 2000. Course: 15-412 Operating Systems: Design and Implementation: Content Scrambling System (CSS): Introduction.

[10] David Dorwin, Jerry Smith, Mark Watson, Adrian Bateman (Eds.). 2017. Encrypted Media Extensions. W3C. Retrieved March 2, 2018 from https://www.w3.org/TR/encrypted-media/

[11] J. Alex Halderman, Edward W. Felten. 2006. Lessons from the Sony CD DRM Episode. Retrieved March 1, 2018 from https://www.copyright.gov/1201/2006/hearings/sonydrm-ext.pdf https://www.copyright.gov/legislation/dmca.pdf.

[12] Mike Williams. 2018. Why isn't a VPN hiding my real location?. Retrieved March 2, 2018 from https://www.techradar.com/news/why-isnt-a-vpn-hiding-my-real-location

[13] Rob Pegoraro. 2011. E-book business should take a page from music industry and go DRM-free. Retrieved March 2, 2018 from https://www.washingtonpost.com/e-book-business-should-take-a-page-from-music-industry-and-go-drm-free/2011/04/05/AFBRbG1C_story.html?utm_term=.6ef672d567d9

P

[redacted]

[redacted]

University of Houston

[redacted]

F: B

C: B-

Presentation completed March 3rd, 2018

not the given title

Fair Use: The Sturdy yet Spindly Bridge between Commoners and Copyrights

Abstract

Fair use is a necessary yet murky doctrine within the Copyright Act that allows users to use copyrighted material without permission. It is perhaps the most significant aspect of the Copyright Act as it potentially can apply to almost every single work that is being protected. However, the fair use doctrine is also extremely murky and broad in its definition and has been subject to numerous controversies and legal cases over the years and has caused frustrations for professionals and commoners alike. When determining whether fair use has been applied in a certain legal case, four factors are explicitly stated and must be applied as well as maybe some other smaller factors. Almost all courts use these factors for determining whether a use is fair. Other scenarios and issues may arise when applying the fair use doctrine, such as the consideration of how it applies through different mediums and potential technological inhibitors. While it is a not a perfect system, the concept of fair use is essential to society as a whole and definitely can have room for potential improvement.

Table of Contents

What is fair use?

The fair use doctrine was included in the Copyright Act of 1976 as a permit for personal and professional use of exclusive copyrighted work without suffering legal ramifications. It is enacted with the intention "to promote science and the arts" while allowing "breathing space within the confines of copyright" since copyright laws generally tend to favor the copyright owners. (Aufderheide 80) Legal fair use of a certain copyrighted work must fall between the categories of "criticism, comment, news reporting, teaching, scholarship, or research" as stated in Section 107 of the Copyright Act, the section that pertains to fair use. ("US Code") However, whether a certain use of copyrighted work is fair or not is deliberately vaguely defined and seems to vary on a case to case basis, with the final decision always resting in the hands of the judges. The big picture of determining fair use always looks at "whether social benefit is greater than private loss." (Aufderheide 24) In determining whether a use is fair or not, the US government devised four major questions, often called "four factors", to reason. Those four factors are: "purpose and character of use", "nature of copyrighted work", "amount and substantiality of the work used", and most importantly, "effect of use on the copyrighted work". ("US Code") These four factors officially became a part of the law in 1978 and has been the standard in legal cases ever since. Although these factors are not considered to be definitive and the factors may vary in weight from case to case, they do provide a roadmap and almost a "scorecard" for guidance on whether to decide a case is fair use or not.

Factor #1: The purpose and character of the use

One of the more important factor of the four, this factor will ask the question "What are you doing with the work?" Most likely this question asks whether the work is used for commercial purposes or nonprofit educational purposes, or more specifically, this factor "asks whether the original was copied in good faith to benefit the public or primarily for the commercial interests of the infringer." (Armatas 114) A work will be considered to be for educational purposes if it falls under the fair use definition of "criticism, comment, news reporting, teaching, scholarship, or research." It is generally presumed that using copyrighted work that is for educational purposes will be fair and for commercial purposes will be presumed unfair. These presumptions are not definitive though. Having a use that is educational in purpose does not guarantee it to be fair and having a use that is commercial in purpose does not guarantee it to be unfair, it merely increases the likelihood in both respective purposes.

However, there are issues with those presumptions. One issue is that on many instances of use has purposes that fits both commercial and educational purposes. It is hard to decide works, such as educational books, are commercial or educational, since most authors can be presumed to hope to gain a commercial profit, or at the very least recognition, for their copyrighted work.

Recent cases that uses this first factor as an analysis has shown that the use of copyrighted work must "involve some qualitative measure of the value generated." (Armatas

114) The term that is commonly used here is whether a work is "transformative" and has been edited enough so that it "makes some contribution of new intellectual value and thereby fostering the advancement of the arts and sciences." (Armatas 115) An example of this concept being applied is the 1994 decision of *Campbell v. Acuff-Rose Music Inc.* In this particular case the music group sued the musician Luke Campbell for using copyrighted music without permission and sold numerous copies of the recording for commercial gain. The Supreme Court that since Campbell's music was a parody of the original work, it is considered to be "transformative" and adds original content, thereby making the use fair under the first factor. In a case like this one, the "transformative" element of the work was taken by the Supreme Court to be more significant and definitive than whether the work was for commercial or education purposes (it was clearly commercial) and the other three purposes.

Another case where whether a use was "transformative" is the 1983 decision of *Marcus v. Rowley.* In this case, one teacher copied almost verbatim the education materials written by another teacher and was taken to court. The court ruled that even though this was done for educational purposes, it was not "transformative" and did not add anything of value to society, hence it was ruled to be not fair use.

There are several other court cases involving schools and other educational purposes that has deemed the use to be unfair since it did not involve any "transformation" of the original work. It is clearly seen that with the significance of the application of the "transformative" concept, that this first factor is a major factor in determining fair use and can sometimes be seen as the most important factor of the four and results in the first factor sometimes being known as "the transformative factor." (Measuring fair use)

Factor #2: Nature of copyrighted work

The second factor is fair use determination will look at the content and protection that has been levied on the work itself. Use of work that involves more factual information, especially historical facts, over fictional works will be much more likely to be considered fair. For example, "no biographer holds a monopoly on the subject's life." (Armatas 116) In fact, facts and ideas aren't not protected by copyrights, only the expression of them are protected in a concept known as the idea-expression divide. Courts will generally protected copyrighted works that involves creativity, such as art, music, poetry, than work that are nonfictional in nature.

Also, using works that are published is more likely to be fair use than using work that is unpublished, since "an author has the right to control the first public appearance of his or her expression." ("Measuring fair use") Those unpublished works that are used should be judged on the laws or privacy, not on the laws of copyright.

One application of this factor can be seen in the court case *Salinger v. Random House Inc.* In this case, a biographer wrote a biography of the famed author J.D. Salinger and used his unpublished letters as a source, which became the key in this legal case. The courts ruled that the use of the unpublished letters without permission is not deemed as fair use. ("Salinger vs Random House")

Factor #3: Amount and Substantiality of the work used

The third factor of the fair use determination is approached from not only a quantitative standpoint but also a qualitative standpoint. It looks how not only the amount of copyrighted work that is being used but also the significance of the portion taken in respect to the work as a whole, which is labelled as the "heart of the work." (Measuring fair use) Generally, using less copyrighted work will be more likely to be considered as fair use, while taking less significant portions of the work will also be more likely to be considered as fair use. Just like the other factors, these definitions are not definitive in determining fair use, and only provide a factor of consideration. So it is very possible in some instances to use 100% of a work and still have it be considered as fair use.

Such is the case in *Sony Corp. of America v. Universal City Studios Inc.* In this case, Universal sued Sony for producing devices that allowed the recording of entire aired programs of Universal, which Sony should be held responsible for. The Supreme Court ruled that even though an entire program can potentially be recorded with the Sony device, it is merely used for the purpose of "time shifting" (using a certain legal work at a different time). (Sony vs Universal) This was considered legal under fair use guidelines.

In some rare cases, the amount of work that is used is so small or so negligible that it does not even require a determination of fair use. This is a rare situation and is known as a de minimis (so small) defense. (Measuring fair use) One example of this defense is the 1998 decision of the case *Sandoval v. New Line Cinema.* In this case, New Line Cinema produced a

movie in which several photographs belonging to Sandoval was used without permission. However, the court ruled that the photos "appear fleetingly and are obscured, severely out of focus, and virtually unidentifiable." (Findlaw) By using a de minimis defense, the court did not even go to a fair use determination and so the photographs were not considered to be infringed.

However, just like many of the other factors of fair use, there is no distinct "line" to determine quantitatively or qualitatively whether a use is fair or not. This factor is also simply another consideration in the final decision of the judges, who always make the final decision on the determination of fair use.

Factor #4: Effect of use on the copyrighted work

The fourth and final factor, which considered by many to be the most important factor, looks at how the use of a copyrighted work affects "not only the current, but potential, value" of a copyrighted work. (Armatas 66) This factors also applies to any derivative of the original work. (Armatas 117) The reasoning behind this factor is that infringed work that is "untransformed" (alluding to factor #1) is considered as a "marketplace substitute" and will harm the market value of the original work. (Armatas 117) Even if an entry of a marketplace has never occurred, use of work will not be considered for fair use because it damages the potential of marketplace entry.

An example of potential market value damage is expressed in the 1992 decision of the case *Rogers v. Koons*. In this case, a sculptor uses a copyrighted photograph without permission to create wooden sculptures. He claimed fair use when the photographer sued because he claims that the photographer would not have used the photograph for a sculpture. The court disagreed with his claim of fair use based on that his use of the photographs hurt the potential value of such a photograph. Even if the photographer had not made a sculpture based on the photo, does not mean that there is no chance the photo is going to be used for the use of a sculpture. (Measuring fair use)

Non-commercial, educational, and transformative works will often be considered as fair use however, even if it does damage the current or potential market value for a copyrighted work.(Armatas 67) One such example of this is the parody or negative review of a certain work, which can drastically reduce and even replace the original work altogether, if the parody is

considered by the audience to be superior to the original work. However this is not considered to be a copyright infringement as a review applies to the very definition of fair use as this is considered to be a form of criticism or comment, and a parody will require the "transformation" of the original work. As one judge explained "the economic effect of a parody with which we are concerned is not its potential to destroy or diminish the market for the original—any bad review can have that effect—but whether it fulfills the demand for the original." (Measuring fair use)

Other Factors

There are also other factors that can weigh into the determination of fair use that are not explicitly stated in any of the four factors. One factor that may be attributed to the broad definition and subjective judgement of the fair use doctrine is the emotional level and moral standard of the judges in court. One example of such is the 1986 decision of the case *Original Appalachian Artworks Inc. v. Topps Chewing Gum Inc.* In this case a manufacturer of cards parodied popular children's dolls with "gruesome and grotesque names and characters." ("Original Appalachian Artworks vs Topps Chewing Gum") Although this was a parody work, the court ruled that this was a copyright infringement.

Two other possible factors may be also considered. A user may have bad or sloppy conduct and not "quote, cite, or even acknowledge" the source after fair use. A user also may accidentally infringe on another's work. Such cases like that without explicit determination will be subjected to the decision of the judges.

Issues and Inhibitors

For a doctrine like fair use that has very loose and informal definitions, the subjective judgement of the court will always be the final say and may differ from case to case, which may lead to many controversial rulings. Even though the court system tries to not emphasize any of the four factors over any other, it has been well known that factor number one and factor number four are the most heavily considered factors. Factor number four has long been considered the most significant factor until 1990 when a federal judge, Pierre Laval, wrote an article *"Toward a Fair Use Standard"* emphasizing the importance of the "transformative" factor. (Laval) Such power in the hands of the judges may weaken checks and balance from the perspective that the lawmakers who enacted the fair use doctrine does not really have a say at all at determining fair use as it was written so loosely.

Another issue arose from the enactment of the Digital Millennium Copyright Act, which created a network of takedown service on the internet which swiftly removes any content which it considers to be copyright infringement without consideration of fair use. The famous "dancing baby case" *Lenz v. Universal Music Corp.* is one such instance in which a YouTube video was quickly taken down without the consideration of fair use. The courts decided that fair use must be taken into account as it is not just a form of infringement defense but a right of users. ("Lenz vs Universal Music Group) However, even with this ruling, it is very difficult to monitor and address the massive numbers of incidents that takes place daily.

inhibitors & DMCA ?

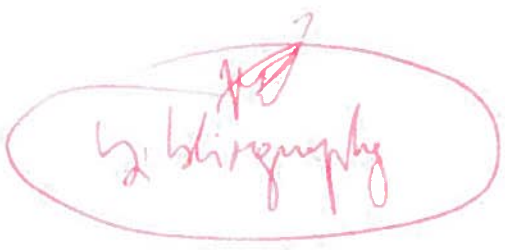
mash-ups ?

Conclusion

The fair use doctrine is one that is created and intended to be ruled on the pillars of the four factors, however it has been described as "so flexible as to virtually defy definition." (Armatas 122) Judges themselves may differ dramatically on the ruling based on the four factors. In one famed Supreme Court case *Harper & Row v. Nation Enterprises*, six of the justices ruled all factors disfavoring fair use, while the other three justices ruled for fair use on all four factors. (Armatas 122)

A study concluded by a scholar of UCLA School of Law David Nimmer produced very surprising results. He analyzed the results 60 different fair use cases and found that on 23 of the 60 cases the losing side won three of the four factors. He even found that on five of those cases the losing side could have potentially won all four factors. This research can clearly see the ineffectiveness of the four factor system and its inability to produce a decisive, undisputable result.

A potentially solution to such a problem can involve mimicking the policies of other nations such as the EU, who has a strict and much more detailed ruling on the issue of fair use. Such a change though, will most likely come as a result of an extremely controversial ruling that is highly publicized or impactful case.



Bibliography

"Sony Corporation of America v. Universal City Studios, Inc." *Oyez*, 3 Mar. 2018, www.oyez.org/cases/1982/81-1687.

Aufderheide, Patricia, and Peter Jaszi. *Reclaiming Fair Use: How to Put Balance Back in Copyright*. The University of Chicago Press, 2018.

"17 U.S. Code § 107 - Limitations on Exclusive Rights: Fair Use." *LII / Legal Information Institute*, www.law.cornell.edu/uscode/text/17/107.https://www.law.cornell.edu/uscode/text/17/107

Armatas, Steven A. *Distance Learning and Copyright: a Guide to Legal Issues*. American Bar Association, 2008.

Leval, Pierre N. "Toward a Fair Use Standard." *Harvard Law Review*, vol. 103, no. 5, 1990, p. 1105., doi:10.2307/1341457.

"Marcus v. Rowley." *Stanford Copyright and Fair Use Center*, 24 Apr. 2013, fairuse.stanford.edu/case/marcus-v-rowley/.

Stim, Richard. "Measuring Fair Use: The Four Factors." *Stanford Copyright and Fair Use Center*, 10 Apr. 2017, fairuse.stanford.edu/overview/fair-use/four-factors/.

"Salinger v. Random House and Ian Hamilton." *Stanford Copyright and Fair Use Center*, 25 Apr. 2013, fairuse.stanford.edu/case/salinger-v-random-house-and-ian-hamilton/.

"FindLaw's United States Second Circuit Case and Opinions." *Findlaw*, caselaw.findlaw.com/us-2nd-circuit/1455045.html.

"Original Appalachian Artworks v. Topps Chewing Gum, 642 F. Supp. 1031 (N.D. Ga. 1986)." *Justia Law*, law.justia.com/cases/federal/district-courts/FSupp/642/1031/2398262/.

"Lenz v. Universal Music Corp." *Harvard Law Review*, harvardlawreview.org/2016/06/lenz-v-universal-music-corp/.

Erin Donnelly

7 March 2018

P

Employers Requiring Applicants, Colleges Requiring Scholarship Recipients to Allow Access to their Social Media Accounts

T: A-
C: A

Abstract

An employer or college attempting to access the social media of an employee or a student has become a fairly common practice, and many will not object to the loss of their privacy to avoid risking their job or their place at a university. In general, social media monitoring in the workplace has more of a spotlight than on college campuses and the ethics and legality can weigh in the employer's favor as the courts tend to do, though states have begun enacting legislation to circumvent this. In colleges, students typically do not bring much legal attention to the issue due to the fear of retaliation, but states are beginning to catch up in enacting legislation in this area as well. This paper explores why employers and colleges seek access to social media, the laws supporting or prohibiting that access, and the ethics surrounding the practice.

Table of Contents

Introduction

Before the rise of social media, most distant social interaction came in the form of letters, telegraphs, and emails. These forms of communication are understood to be private, and this privacy is enforced by the illegality of opening another person's letters and encryption protecting digital communications such as email. However, with the popularization of the more public social media, communications and other aspects of private life are more accessible to those outside of a person's intended audience. Sociologist Erving Goffman proposed that individuals give "multiple life performances" [2] in front of different audiences. For example, they will act differently in front of their friends versus in front of their boss. For the multiple life performances to retain their validity, the audiences must be kept segregated. If a person acted their 'friends' performance in front of their boss, then the boss's perception of their 'professional' persona would fall apart. Traditional professionalism demands that individuals keep their work and school performances separate from their private life, but this professionalism can't be kept intact if employers begin delving into their employees' private lives via social media [2]. Goffman wrote about these ideas in 1959, and they are surprisingly applicable today with the advent of social media.

Some important privacy terms surrounding the issue of social media access include 'reasonable expectation of privacy' and 'search.' Having a reasonable expectation of privacy does not automatically mean that a person has a right to privacy. The court case Katz v. United States set a precedent for a two-part test for the right to privacy. In the case, a phone booth Katz was using to make a call was eavesdropped on by federal agents, who convicted him of illegal transmission of wagering information based on the recordings they picked up [14]. The Supreme Court ruled that Katz was entitled to the protection of his conversations via the Fourth

Amendment. The court also decided that to have a right to privacy, the individual must first have a subjective expectation of privacy, which can be proven by seeking to preserve his or her privacy, and then that expectation must be recognized as reasonable by society [2]. Also note that Katz v. United States also established a "search" to be an intrusion by a government official into a constitutionally protected area where one has a reasonable expectation of privacy with the intent of obtaining information [2].

A few pieces of legislature continually crop up in court cases surrounding social media monitoring. The First Amendment, which protects freedom of speech, the Fourth Amendment, which protects against unreasonable search and seizure, and the Electronic Communications Privacy Act (ECPA). The ECPA has two titles of note: The Wiretap Act prohibits the interception, use, and disclosure of communications in transit, and the Stored Communications Act (SCA) prohibits the intentional and unauthorized use of stored communications. The Wiretap Act has significant exceptions which limit its applicability to monitoring and surveillance of social media. One exception is that it does not apply to communications made through a publicly available communication system, a second is an exception for providers of a communication service, and a third permits interception of communication if one party gives explicit or implicit consent [2]. Therefore, an employer who finds communications posted online publicly, provides his employee with a cell phone or Internet access, or obtains consent from an employee through an electronic communications policy or contract clause can legally access their employee's communications on these platforms [2]. On the other hand, the SCA appears in many court cases surrounding the monitoring issue because while it still excludes a few parties from liability like the intended recipient of the communication or those allowed access by the

communication service provider, it can protect employees whose online information was accessed in an unauthorized manner [2].

Employers and their Motivations

Employers typically attempt to view employees' or candidates' social media by asking a candidate to log in to his social media during an interview, or requiring login information or the acceptance of a friend request from a superior from an employee or candidate. These controversial techniques come from desires to protect their reputation, screen potential new employees, avoid lawsuits, and mitigate the insider threat.

A company's reputation and assets lie on the line when it allows its employees to post information without monitoring. It is well known that a disgruntled employee can easily cause harm to his company by disclosing intellectual assets or tarnishing names and products online, but even a well-intentioned employee could accidentally divulge evidence of their company's negligence, immorality, or incompetence [2]. By monitoring social media, they can decrease the risk of both of these occurrences.

Employers also want to avoid hiring employees with poor character. In 2017, CareerBuilder surveyed over 2300 hiring managers and HR professionals across industries and company sizes in the private sector. They found that 70% used social media to screen candidates, 24% of those look for a reason *not* to hire a candidate, and over half of them found a reason not to hire a candidate [3]. Additionally, 57% are less likely to call in a candidate for an interview if they cannot be located online, and on the job, 34% found content on social media leading to a reprimand or firing of an employee [3]. Each of these statistics shows the substantial role social media plays when employers decide which employees to hire and fire. To be fair to the

employer, however, many of the reasons they cite for dismissing an applicant or employee are good ones: some of the reasons stated are the participation in illegal activities, lying, and making discriminatory comments [3].

Employers also try to avoid lawsuits by screening via social media. Failing to uncover an obvious flaw in an employee's background and character can lead to negligent hiring lawsuits, where a third party was harmed and the employer knew the risk or could have known through reasonable investigation, and negligent retention lawsuits, which are similar but related to the retention of a risky employee [2]. For example, in Doe v. XYC Corp., an employer faced liability for his employee who had posted nude pictures of his daughter using a company computer [2]. These lawsuits could have serious business repercussions, so employers have a strong motivation to learn about their employees' morals and personalities so they can avoid situations where they may be liable for a morally-deficient or criminally-inclined employee [2].

Lastly, employers wish to mitigate the insider threat. The insider threat refers to an employee who deliberately works against the company while employed. The current methods of insider detection, like risk assessment and communications monitoring, only attempt to collect and analyze hard data, without aggregating in the "human factor," or traits about the individual's personality [1]. Traits like narcissism, divided loyalty, and a disposition against law enforcement are common among insider threats, and these traits can be detectable on social media [1]. If employers supplemented their current methods of detection with social media monitoring, they could have an edge on detecting insiders.

Employers: Legality

There are some legal issues associated with the monitoring of employee social media. In favor of the employer is noting that the workplace and resources are the property of the employer, but some other issues such as the ECPA's influence on the legality of monitoring, the possibility of illegal discrimination, and the suppression of free speech in the workplace call the legality of the practice into question.

Courts typically agree that the workplace and its resources are the property of the employer. In a lawsuit, the burden of proving a reasonable expectation of privacy in the workplace lies on the employee, although courts usually favor the employer anyways [2]. In addition, courts generally rule that employees have no privacy expectations in the workplace (barring some exceptions), and that employers have a legitimate interest in monitoring social media and other communications [2].

Some exceptions to the court's recommendation for employees not to expect privacy lie in the ECPA. Accessing information is legal if it is public, but illegal if access to password-protected information is obtained in an unauthorized way (surreptitiously or by coercion) because it violates the SCA [2]. In Pietrylo v. Hillstone Restaurant Group, a few employees shared a MySpace page to vent about their employer. Eventually one employee, the hostess, gave her login information to a manager who promptly fired the involved employees. When the hostess testified, she claimed that she was coerced to give the login information and the court found that the employer violated the SCA [2]. In another court case, Pure Power Boot Camp v. Warrior Fitness Boot Camp, an employee stored his password on a company computer, which the employer found and used to access his non-work-related Gmail account. The courts also

found this as a violation of the SCA, ruling that the employee did have a reasonable expectation of privacy in storing his passwords on the computer despite it belonging to the company [2].

Monitoring also opens the possibility of illegal discrimination. Employers are not required by law to disclose social background checks, so if applicants are never called back due to something on their social media, they have no way of defending themselves [2]. Additionally, while we know typical discrimination categories to be age, sex, gender, etc. many states broaden the scope to include things like legal recreational activities, political activities, and consumption of legal products [2]. Because employers don't have to disclose the information they find, they could easily discriminate based on anything they would like to in the moment.

Regarding employee speech rights, the Supreme Court holds that if employees are in the course of official duties, they have no protection, and if they are outside of work, they may still be penalized depending on the situation [2]. They decide on this by weighing employer business interests with free expression, and courts will commonly rule in favor of business interests. In City of San Diego v. Roe, a police officer sold videos of himself stripping and performing sexual activities. The officer was promptly fired. The court ruled that though he was off-duty at the time, his activities were sufficiently linked to his employment and detrimental to his employer so his employer could lawfully fire him [2].

Employers: Ethicality

Moving on to ethical issues in monitoring social media, monitoring reduces trust between the employer and employee, suppresses the employee's personality and freedom of speech, correlates with higher levels of mental illness and fatigue, and can allow for unjustified profiling.

Naturally, if an employer feels the need to monitor an employee, the employee would assume that he is not trusted. In fact, 75% of millennials find monitoring a breach of employee-employer trust [2]. While employers have their companies' best interests at heart when they monitor social media, the subsequent decrease in trust could end up hurting the company anyways. A 2014 study showed that the level of trust between employees and employers can influence the extent to which employees engage in opportunistic behavior, as well as influencing the productivity and performance of employees in the workplace [4]. Without trust, more opportunities may be taken that will damage the company, and productivity and performance could suffer.

Suppressing personality and free speech ends up being detrimental to the employer as well. Audiences can't be kept separate if employers force themselves onto friends-and-family platforms, so employees are forced to keep a professional performance even off duty. Harvard Business review found that some discomfort in the workplace increases creativity, but if that discomfort extends into fear, then the employee's drive for self-protection is increased and he will only care about playing it safe [11]. A study by Adobe found that companies who foster creativity are 3.5 times more likely to achieve revenue growth of over 10% and more likely to be market leaders as well [10].

Monitoring communications also correlates with higher levels of depression, anxiety, fatigue, and physical pain. A two-year study at the University of Wisconsin found that workplace monitoring increased depression by 12% and extreme anxiety by 15% [12]. Therefore, employers must decide if monitoring is worth the risk of harming their employees' mental and physical well-being.

For the last of the ethical issues, in monitoring applicants, employers will likely assign individuals to categories because it is easier to make a decision based on a category than on a complex individual. In profiling candidates, they try to figure out what "sort of person" [5] someone is instead of looking at them as an individual. The information on social media is also typically job-irrelevant and for a different audience, and the conclusions that the employer draws may or may not be true.

Colleges and their Motivations

To address colleges and their monitoring of social media, a clarification must be made. Though college applicants are sometimes screened via social media, the brunt of social media scrutiny is focused on athletes. As faces of the university, athletes are often required to friend coaches who can dole out punishments such as suspension, dismissal from the team, or non-renewal of aid if they find any non-approved posts. The National Collegiate Athletic Association has three divisions. Division I is composed of large universities with the highest athletic budgets and 59% of athletes belonging to that division receive some sort of financial aid [13]. In Divisions II and III the percentages are higher at 60 and 80% [13]. This means that a clear majority of athletes receive a scholarship or grant from their school and are subsequently subject to social media restrictions.

The rationales colleges make for monitoring athletes' social media are that the athletes willingly forgo freedom in exchange for benefits, that athletics is akin to employment, and that they need to protect the institution and athlete from poor public image.

Colleges claim that athletic participation is a privilege and that their rights can be forfeited for the ability to play or for other benefits such as financial aid. In contrast, the court

case Thomas v. Review Board found that a citizen can't be compelled to forsake his first amendment rights in exchange for benefits [7]. Thomas was an employee of a manufacturing company who moved him to weapons manufacturing. This conflicted with his religion so he asked to be laid off but was refused, so he quit. He was denied unemployment compensation due to his reason for quitting, but that decision was reversed when the case hit the Supreme Court who protected his first amendment rights and decided that he was owed unemployment compensation despite his reasoning [7].

Colleges also claim that athletic participation is analogous to employment. As a reminder, employers can legally discipline unprofessional job-related speech. However, there are legal consequences for classifying athletes as employees, including a responsibility to pay worker's compensation or spousal death benefits, which colleges most likely will not want to pay [7].

Lastly, colleges also want to protect themselves and their athletes from poor public image, which may cause headaches or other consequences for both parties. However, in a government setting, imposing a penalty on free speech for this reason would be readily be considered unconstitutional [7].

Colleges: Legality

As for legal issues, social media monitoring at the college level constitutes an unreasonable search and violates freedom of expression, and colleges also take on unnecessary legal liability when they monitor.

The court has interpreted the fourth amendment to include a prohibition of searches by public school officials. Additionally, there was a court case that emphasized the role of consent in a search. In Bumper v. North Carolina, law enforcement was investigating a man and searched

his grandmother's house where he was currently living. His grandmother consented only after officials told her they had a warrant, which was a lie [15]. The evidence the officials found was deemed inadmissible because the Supreme Court found that an involuntary search, even with consent, is an unreasonable search because consent is not voluntary if it is achieved under duress or coercion [15]. Since most athletes give up privacy in their social media based on the assumption there would be punishments or other consequences for not doing so, their consent could be considered coerced.

The monitoring also violates freedom of expression. The decades-old court case Tinker v. Des Moines Indep. Cmty. Sch. Dist. decided that First Amendment rights were not waived upon entering a public school after students were punished for protesting the Vietnam war by wearing black armbands [7]. This set the precedent that students have freedom of speech in public schools as long as it doesn't disturb the teaching environment [7]. Unless athletes disrupt the teaching environment on social media, which would be a complicated feat, they should have a right to express themselves as they wish.

An issue that isn't frequently considered is that if schools begin aggressively monitoring students' social media, they may become liable for any crimes that occur when warning signs were given online [8]. In the 2010 Yeardley Love case, a male lacrosse player at the University of Virginia murdered a female lacrosse player [8]. If the college had seen the warning signs on his social media, they could have been liable to put a stop to it, like in employer negligence lawsuits where the employer does not take action when an employee proves to be a risk to others.

Colleges: Ethicality

Lastly, there are ethical concerns when colleges try to monitor social media, including forced consent when students are afraid of retaliation, the fact that athletes typically have difficulty seeking lawsuits, and the fact that enforcing authorities are the ones who decide what 'offensive' language is.

The term "forced consent" [6] applies when consent is demanded with the implication that there will be retaliation if the athlete does not agree. Schools can easily penalize athletes by revoking play privileges or scholarships if athletes will not consent. This is similar to the fourth amendment's declaration that consent under duress/coercion constitutes an unreasonable search. However, in consistency with the ruling that the First Amendment protects students up until the teaching environment is disturbed, courts usually rule in favor of forced consent when teachers need to maintain discipline at school [6].

Athletes also have trouble seeking lawsuits for a few reasons. First, the athlete may graduate or transfer while the case is still pending, making it useless to continue for the most part [7]. He or she may have trouble demonstrating financial loss, for if they argue that the lack of playtime diminished their chances of going professional, only a small percentage of players go on to be professional anyways [7]. Also, the athlete may wish to retain their position on the team or keep their relations with the coach and not risk rocking the boat by pursuing a lawsuit [7].

The first amendment does not extend to some profanity, threats, or "bad tendency" [6] speech (speech with a tendency to cause violence or crime), but aside from this, there are no standards as to what can be posted online. As with the employer deciding whether or not they like someone's social media profile, the judgment of an athlete's content is solely based on the subjective whims of the enforcing authority [6].

State Legislation

Since 2012, states have begun introducing legislation attempting to prevent employers and institutions from requesting login information to employees' and students' social media. So far, 26 states (plus Guam) have created laws that apply to employers; 15 of these have also created laws that apply to institutions, as well as the District of Columbia, which does not currently have a law for employers [16].

The first state to successfully pass legislation protecting against social media intrusion was Maryland, whose governor signed a law in May of 2012 prohibiting an employer from requesting that an employee divulge thei login information for a personal account or service. By the end of the year, 6 states (California, Delaware, Illinois, Maryland, Michigan and New Jersey) passed legislation and 8 more states introduced legislation protecting an employee, student, or applicant from being required to disclose their usernames and passwords. In 2013, legislation was introduced or considered in at least 36 states while 10 of those enacted legislation. In 2014, 7 more enacted legislation, and 9 in 2015 amounting to nearly half of the U.S. states. In 2016, legislation slowed, with 4 states passing laws, and in 2017 there were only 2. In total, all states but two, Idaho and Kentucky, have attempted legislature [16].

Of the legislature that was passed, many set prohibitions on both asking and requiring access to an employee's or student's social media, while some only explicitly prohibit requiring. A few have exceptions, for example Illinois allows a school to request or require social media login information if the school believes that the student's account shows evidence of the student violating a rule or policy. Some, such as Oklahoma and Nebraska, specifically state that employers and schools cannot retaliate against an employee or student for not consenting to give access to their social media [16]. Despite some differences in the wording and the exceptions,

most states seem to aim to protect employees and students from an employer or institution who wishes to gain access to their social media.

Conclusions

In both workplaces and at schools, privacy is traded for something of value. Employees and students agree to requests for access to social media in hopes for a favorable outcome such as getting or keeping a job, or playing sports. Employers and colleges also have some similar motivations, such as protecting their reputation from things a subordinate may say.

In conclusion, employers tend to have stronger rationales and legal protections for monitoring employees, but they could be harming themselves as far as performance and production in the workplace. On the other hand, colleges have fewer rationales and are on a more uncertain legal footing, and mostly protected by the athletes' unwillingness to sue.

Bibliography

1. Dimitris Gritzalis, Vasilis Stavrou, Miltiadis Kandias and George Stergiopoulos, "Insider Threat: Enhancing BPM through Social Media," 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), Dubai, 2014, pp. 1-6. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6814027&isnumber=6813963
2. Sánchez Abril, P., Levin, A. and Del Riego, A. (2012), "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee." Am Bus Law J, 49: 63–124. doi:10.1111/j.1744-1714.2011.01127.x
3. "Number of Employers Using Social Media to Screen Candidates at All-Time High, Finds Latest CareerBuilder Study." PR Newswire: News Distribution, Targeting and Monitoring, 14 June 2017, www.prnewswire.com/news-releases/number-of-employers-using-social-media-to-screen-candidates-at-all-time-high-finds-latest-careerbuilder-study-300474228.html.
4. Sarah Brown, Daniel Gray, Jolian McHardy, Karl Taylor, "Employee trust and workplace performance," Journal of Economic Behavior & Organization, Volume 116, 2015, Pages 361-378, ISSN 0167-2681, https://doi.org/10.1016/j.jebo.2015.05.001. (http://www.sciencedirect.com/science/article/pii/S0167268115001365)
5. Miltiadis Kandias, Lilian Mitrou, Dimitris Gritzalis. "Social Media Profiling: a Panopticon or Omniopticon Tool?" 6th Biannual Surveillance and Society Conference, Barcelona, 2014. URL: http://www.ssn2014.net/?page_id=1609.
6. Talon Hurst. "Give Me Your Password: The Intrusive Social Media Policies in Our Schools," 22 CommLaw Conspectus 196 (2014). Available at: https://scholarship.law.edu/commlaw/vol22/iss1/9

7. Frank LoMonte. "College Sports and Social Media: Leave Your Rights in the Locker Room?" American Bar Association. URL: https://apps.americanbar.org/litigation/committees/civil/articles/spring2014-0514-college-sports-social-media-leave-your-rights-locker-room.html. Accessed 5 March 2018.

8. Aaron Kasinitz. "Colleges Monitor, Restrict Athletes on Social Media." American Journalism Review. 26 March 2014. URL: http://ajr.org/2014/03/26/social-media-monitoring-widespread-among-college-athletic-departments/. Accessed 5 March 2018.

9. Bob Sullivan. "Govt. agencies, colleges demand applicants' Facebook passwords." NBCNews. 6 March 2012. URL: https://www.nbcnews.com/business/consumer/govt-agencies-colleges-demand-applicants-facebook-passwords-f328791. Accessed 5 March 2018.

10. "It's official: Creativity drives business results." Adobe Creative Cloud, landing.adobe.com/en/na/products/creative-cloud/55563-creative-dividends.html?scid=social32176426.

11. Levirne, Jake. "The Most Overlooked Way of Stimulating Team Creativity." Harvard Business Review, 15 May 2015, hbr.org/2015/05/the-most-overlooked-way-of-stimulating-team-creativity.

12. Julie A. Flanagan. "Restricting Electronic Monitoring in the Private Workplace." 43 Duke Law Journal 1256-1281 (1994). Available at: https://scholarship.law.duke.edu/dlj/vol43/iss6/6

13. https://www.ncaa.org/sites/default/files/Recruiting%20Fact%20Sheet%20WEB.pdf

14. "Katz v. United States." Oyez, 6 Mar. 2018, www.oyez.org/cases/1967/35. Accessed 6 March 2018.

15. "Bumper v. North Carolina." Oyez, 6 Mar. 2018, www.oyez.org/cases/1967/1016. Accessed 6 March 2018.

16. "Access to Social Media Usernames and Passwords." National Conference of State Legislatures. http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx. Accessed 6 March 2018.