

Encryption and the Law



Protecting Innovation by Supporting Student Research and Discovery

The BU/MIT Technology & Cyberlaw Clinic is a *pro bono* service for students at MIT and BU who seek legal assistance with their innovation-related academic and extracurricular activities. Boston University School of Law students, under attorney supervision, provide counseling and representation to students with their academic- and innovation-related projects, activities, experiments, and ventures.

The Technology & Cyberlaw Clinic is part of a collaboration between Boston University School of Law and the Massachusetts Institute of Technology. Along with its companion clinic — the [Entrepreneurship & Intellectual Property Clinic](#), which provides legal advice to startups coming out of MIT and BU — BU Law students are given an opportunity to work on cutting-edge issues of technology law, while students at both universities can obtain legal guidance and assistance with their research.



Encryption and the Law

Today – Encryption research and the law

- Anticircumvention law
- The Computer Fraud and Abuse Act
- Contracts
- Code, speech, and the First Amendment

Wednesday – Encryption law and policy

- Limits on encryption of communications
- Lawful surveillance
- “Going dark” and the obligation to decrypt
- Export control and encryption

“Anticircumvention Law” (the law that governs DRM)

“Anticircumvention Law” (the law that governs DRM)

1. Governs access to the underlying content, instead of access to the computer itself.
2. Almost nothing to do with copyright law.

“Normal” copyright

“Normal” copyright

[Congress shall have the power] To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries

“Normal” copyright

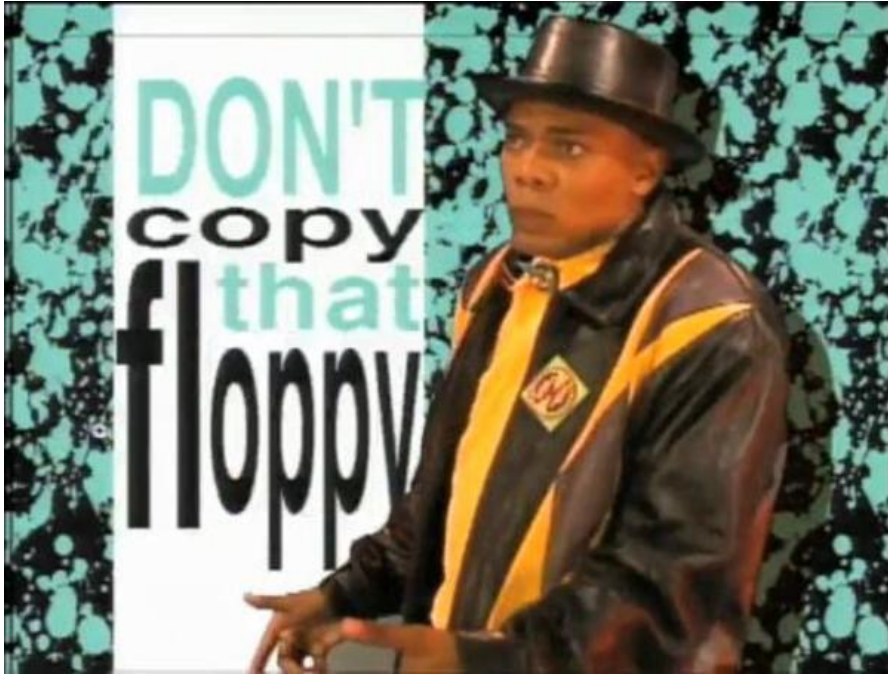
[Congress shall have the power] To promote the Progress of Science and useful Arts, by securing for **limited Times** to **Authors** and Inventors the **exclusive Right** to their respective **Writings** and Discoveries

“Normal” copyright

[Congress shall have the power] To promote the Progress of Science and useful Arts, by securing for **limited Times** to **Authors** and Inventors the **exclusive Right** to their respective **Writings** and Discoveries

- Literary works
- Musical works
- Dramatic works
- Choreographic works
- Pictorial, graphic, and sculptural works
- Audiovisual works
- Sound recordings
- Architectural works
- Reproduction
- Distribution
- Derivative works
- Public performance (not sound recordings)
- Public display
- Digital audio transmission (sound recordings only)
- Limited (but long!) duration
- Statutory carveouts and blanket licenses
- Fair use
- Judicial interventions

“Normal” copyright



“Normal” copyright



“Anticircumvention”

“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”

(encryption is this)

“No person shall circumvent **a technological measure** that effectively controls access to **a work protected under this title.**”

(software is this)

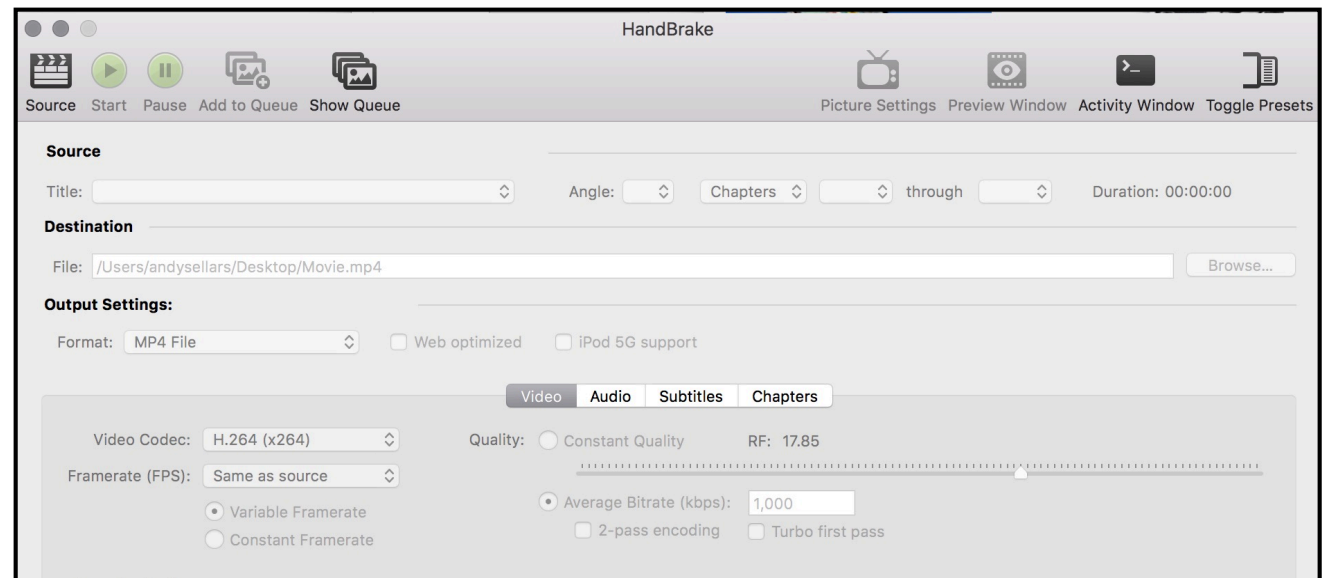
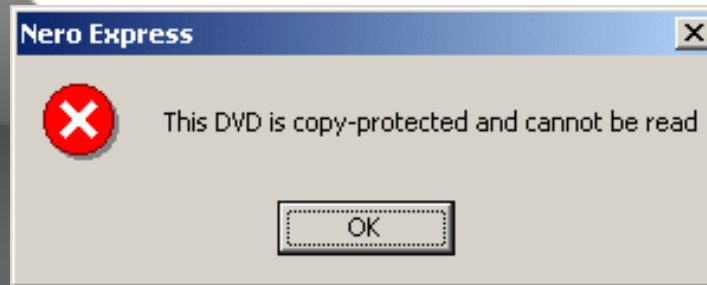
	Access Protection	Rights Protection (e.g., disabling copying, eliminating outputs, degrading copies)
Individual Circumvention	prohibited, subject to some permanent and some evolving exceptions (§ 1201(a)(1)(A))	not addressed by DMCA (per legislative history, governed by copyright law itself)
Making or Offering Devices that Circumvent	prohibited if primarily designed to do so, or if marketed to do so, or if it has limited purpose other than to circumvent (§ 1201(a)(2))	prohibited if primarily designed to do so, or if marketed to do so, or if it has limited purpose other than to circumvent (§ 1201(b))

“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”

(3) As used in this subsection—

(A) to “circumvent a technological measure” means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

(B) a technological measure “effectively controls access to a work” if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.







I'm not a robot



reCAPTCHA

[Privacy](#) - [Terms](#)



Terms of Service

Community Guidelines

1. Your Acceptance

- A. By using or visiting the YouTube website or any YouTube products, software, data feeds, and services provided to you on, from, or through the YouTube website (collectively the "Service") you signify your agreement to (1) these terms and conditions (the "Terms of Service"), (2) Google's Privacy Policy, found at <https://www.youtube.com/t/privacy> and incorporated herein by reference, and (3) YouTube's Community Guidelines, found at https://www.youtube.com/t/community_guidelines and also incorporated herein by reference. If you do not agree to any of these terms, the Google Privacy Policy, or the Community Guidelines, please do not use the Service.
- B. Although we may attempt to notify you when major changes are made to these Terms of Service, you should periodically review the most up-to-date version <https://www.youtube.com/t/terms>). YouTube may, in its sole discretion, modify or revise these Terms of Service and policies at any time, and you agree to be bound by such modifications or revisions. Nothing in these Terms of Service shall be deemed to confer any third-party rights or benefits.

2. Service

- A. These Terms of Service apply to all users of the Service, including users who are also contributors of Content on the Service. "Content" includes the text, software, scripts, graphics, photos, sounds, music, videos, audiovisual combinations, interactive features and other materials you may view on, access through, or contribute to the Service. The Service includes all aspects of YouTube, including but not limited to all products, software and services offered via the YouTube website, such as the YouTube channels, the YouTube "Embeddable Player," the YouTube "Uploader" and other applications.





You have been banned!

Account banned for 1 day due to offensive or inappropriate behavior. Repeated offences will lead to a permanent ban.

Okay

Loading

The Lightning Spell damages units and buildings in a small area.



“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”

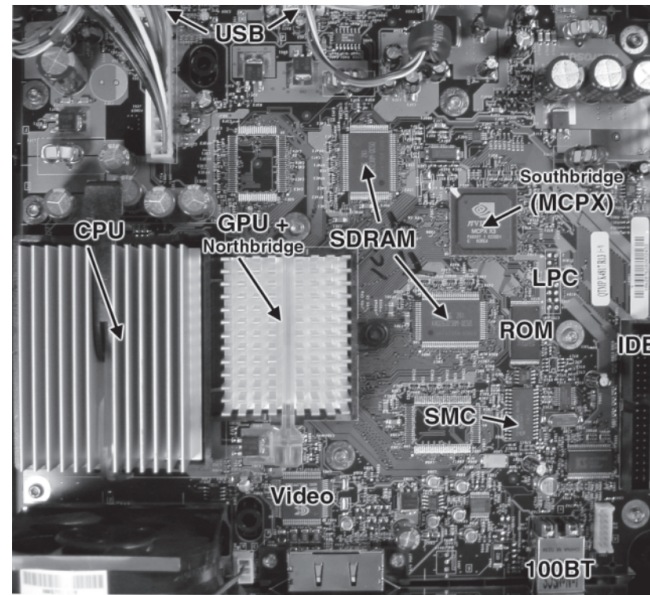
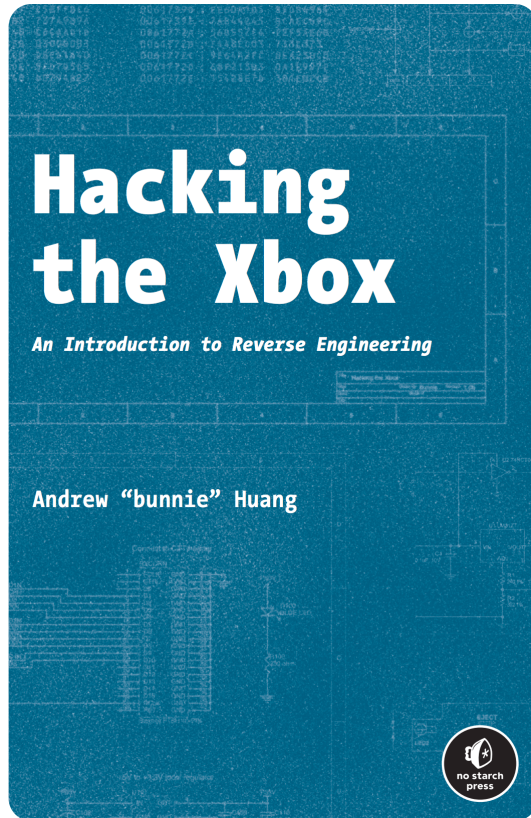


Figure 2-6: Photograph of an Xbox motherboard with the major components labelled.

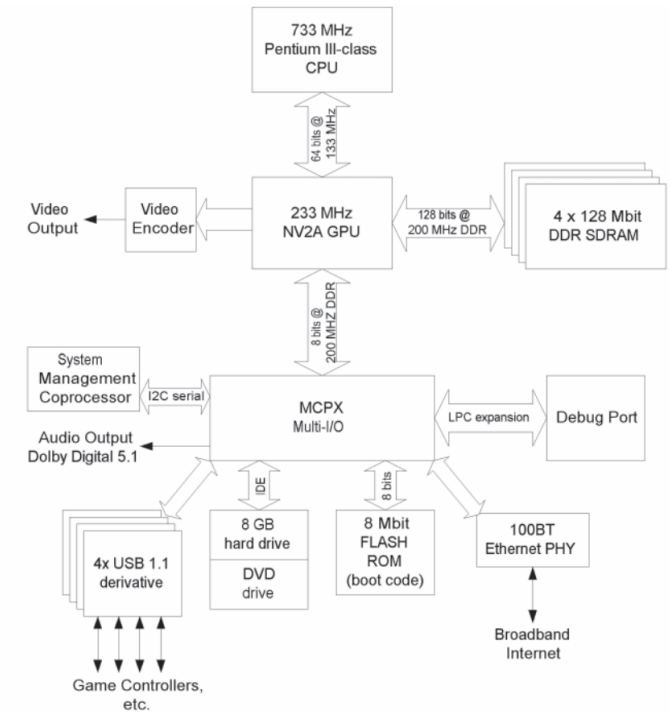


Figure 2-5: High level architectural view of the Xbox.



Exceptions

- § 1201(f) – Reverse Engineering
- § 1201(g) – Encryption Research
- § 1201(j) – Security Research
- Triennial Petitions to the Copyright Office

Exceptions

Good news

You may can circumvent a TPM to analyze a program to achieve interoperability with another program.

- **§ 1201(f) – Reverse Engineering**
- § 1201(g) – Encryption Research
- § 1201(j) – Security Research
- Triennial Petitions to the Copyright Office

Bad news

Must be your “sole purpose,” information must not otherwise be available, and only for achieving interoperability with “an independently created computer program”

Exceptions

- § 1201(f) – Reverse Engineering
- **§ 1201(g) – Encryption Research**
- § 1201(j) – Security Research
- Triennial Petitions to the Copyright Office

Good news

Can circumvent TPM for “encryption research”

Bad news

Must demonstrate that it is done to “advance the state of knowledge in the field of encryption technology,” must be necessary for research, must try and obtain authorization before circumvention. Courts adopt an onerous test to see if bona fide research.

Exceptions

In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

research.

Exceptions

Good news

Can circumvent TPM for “security testing” of a computer system

- § 1201(f) – Reverse Engineering
- § 1201(g) – Encryption Research
- **§ 1201(j) – Security Research**
- Triennial Petitions to the Copyright Office

Bad news

Must have permission from owner of computer, must be to address a flaw in the “computer, computer system, or network.” Courts again look to how the information was used to see if this was done in good faith.

Exceptions

Good news

Can be whatever you want it to be!

- § 1201(f) – Reverse Engineering
- § 1201(g) – Encryption Research
- § 1201(j) – Security Research
- **Triennial Petitions to the Copyright Office**

Bad news

You have to convince the Copyright Office, Department of Commerce, and Librarian of Congress that the exemption should exist.

Exceptions

- § 1201(f) – Reverse Engineering
- § 1201(g) – Fair Use Research
- § 1201(i)

Try
Co



Sept. 2014


LIBRARY OF CONGRESS
U.S. Copyright Office
37 CFR Part 201
[Docket No. 2014-07]

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

AGENCY: U.S. Copyright Office, Library of Congress.
ACTION: Notice of inquiry and request for petitions.

SUMMARY: The United States Copyright Office is initiating the sixth triennial rulemaking proceeding under the Digital Millennium Copyright Act, concerning possible exemptions to the Act's prohibition against circumvention of technological measures that control access to copyrighted works. The Copyright Office invites written petitions for proposed exemptions from interested parties. Unlike in previous rulemakings, the Office is not requesting the submission of complete legal and factual support for such proposals at the

Nov. 2014

 **CYBERLAW CLINIC**
Harvard Law School | Berkman Center for Internet & Society

BEFORE THE UNITED STATES COPYRIGHT OFFICE
LIBRARY OF CONGRESS

PETITION OF A COALITION OF MEDICAL DEVICE RESEARCHERS FOR EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES
Docket No. 2014-07

Submitted by:
Andrew F. Sellars
Cyberlaw Clinic
Berkman Center for Internet & Society
Harvard Law School
23 Everett Street, Second Floor
Cambridge, MA 02138
asellars@cyber.law.harvard.edu

A coalition of medical device patients and researchers (the "Medical Device Research Coalition") submits this petition in response to the Notice of Inquiry on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 79 Fed. Reg. 55,687 (Sept. 17, 2014).

Brief Overview of the Exemption
The members of the Medical Device Research Coalition study the safety, security, and effectiveness of networked medical devices that are either implanted or attached to the body. This Coalition includes researchers who study device security at the design level, as well as those who study the safety and effectiveness of devices they personally use. Such research often requires the researcher to access the underlying source code and outputs from these devices, and device manufacturers are increasingly employing technologies that courts may classify as technological protection measures under § 1201 of the Copyright Act. In order to make sure that this form of critical research continues, the Medical Device Research Coalition proposes the following exemption:

Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is at the

¹ This coalition includes Hugo Campos, Stanford Medicine X; Jerome Radcliffe, Rapid7; Karen Sandler, Software Freedom Conservancy; and Benjamin West, an independent device researcher. The institutional affiliations provided here are for identification purposes only.

1 of 5

Dec. 2014

LIBRARY OF CONGRESS
Copyright Office
37 CFR Part 201
[Docket No. 2014-07]

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

AGENCY: U.S. Copyright Office, Library of Congress.
ACTION: Notice of proposed rulemaking.

SUMMARY: The United States Copyright Office is conducting the sixth triennial rulemaking proceeding under the Digital Millennium Copyright Act, concerning possible exemptions to the Act's prohibition against circumvention of technological measures that control access to copyrighted works.

3. Proposed Class 27: Software—Networked Medical Devices

The proposed class would allow circumvention of TPMs protecting computer programs in medical devices designed for attachment to or implantation in patients and in their corresponding monitoring devices, as well as the outputs generated through those programs. As proposed, the exemption would be limited to cases where circumvention is at the direction of a patient seeking access to information generated by his or her own device, or at the direction of those conducting research into the safety, security, and effectiveness of such devices. The proposal would cover devices such as pacemakers, implantable cardioverter defibrillators, insulin pumps, and continuous glucose monitors.

Feb. 2015

March 2015

BEFORE THE UNITED STATES COPYRIGHT OFFICE
LIBRARY OF CONGRESS

LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. § 1201
Docket No. 2014-07

COMMENT OF A COALITION OF MEDICAL DEVICE RESEARCHERS
IN SUPPORT OF PROPOSED CLASS 27: SOFTWARE – NETWORKED MEDICAL DEVICES

Multimedia evidence is not being provided in connection with this comment.

Pursuant to the Notice of Proposed Rulemaking for Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies¹ (“NPRM”), a Coalition of Medical Device Researchers² (the “Coalition”) submits the following comment and respectfully requests the Copyright Office to recommend Proposed Class 27 for exemption pursuant to 17 U.S.C. § 1201(k)(1)(C).

I. Commenter Information

These comments are submitted by the Coalition through their counsel:

Andrew F. Sellars
Clinical Fellow, Cyberlaw Clinic
Berkman Center for Internet & Society
Harvard Law School
23 Everett Street, Second Floor
Cambridge, MA 02138
(617) 384-9125
asellars@cyber.law.harvard.edu

II. Proposed Class Addressed

These comments relate to Proposed Class #27: Software – Networked Medical Devices.³ In its initial petition, the Coalition proposed the following language for the exemption:

Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is at the direction of a patient seeking access to information generated by his or her own device or at the direction of those conducting research into the safety, security, and effectiveness of such devices.

¹ 79 Fed. Reg. 73,856 (Dec. 12, 2014) [hereinafter NPRM].
² The members of this Coalition are listed in Appendix A.
³ See NPRM, *supra* note 1, at 73,871.



FREE SOFTWARE
FOUNDATION

Comment Regarding a Proposed Exemption
Under 17 U.S.C. 1201

Commenter Information

Dr. Matthew D. Green, PhD, is an Assistant Research Professor in the Department of Computer Science at Johns Hopkins University. He is represented by the Samuelson-Glushko Technology Law & Policy Clinic (TLPC) at the University of Colorado Law School, including Chelsea E. Brooks, Student Attorney, Joseph N. de Raismes, Student Attorney, Andy J. Sayler, Student Technologist, and Prof. Blake E. Reid, TLPC Director.

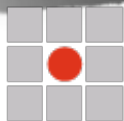
Short Comment Regarding a F

Item 1. Commenter Informa

Jay Freeman (saurik); +1 (805) 895-7209; saurik@saurik.com; SaurikIT, LLC (Member)
Mailing Only: 8605 Santa Monica Boulevard #21162; West Hollywood, CA 90069, USA

Item 2. Proposed Class Addressed

Proposed Class 27: Software – networked medical devices



Public Knowledge



AdvaMed

Advanced Medical Technology Association



JAY SCHULMAN
ME@JAYSCHULMAN.COM

March 27, 2015

In re: Notice of Inquiry on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 79 Fed. Reg. 55,687 (Sept. 17, 2014). Exception for Class 27.

I am currently a Medical Device Researcher working directly with medical device manufacturers to test the security of medical devices through my employer. Under normal circumstances, I'm a proponent of allowing security researchers to test devices. Independent researchers conducting research on their own time have made many significant security findings. But with medical devices, the circumstances are different.



NATIONAL ASSOCIATION OF
Manufacturers



School of Law

Technology & Cyberlaw Clinic

May 2015

BEFORE THE UNITED STATES COPYRIGHT OFFICE
LIBRARY OF CONGRESS

REPLY COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. § 1201
DOCKET NO. 2014-07

REPLY COMMENT OF A COALITION OF MEDICAL DEVICE RESEARCHERS
IN SUPPORT OF PROPOSED CLASS 27: SOFTWARE – NETWORKED MEDICAL DEVICES

Multimedia evidence is not being provided in connection with this comment.

Pursuant to the Notice of Proposed Rulemaking for Exemption to Prohibition on Circumvention of Copyright Protection System for Access Control Technologies,¹ the Coalition of Medical Device Researchers² (the “Coalition”) submits the following reply comments to provide additional legal and factual support regarding:

Proposed Class 27: Software – Networked Medical Devices. Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is at the direction of a patient seeking access to information generated by his or her own device or at the direction of those conducting research into the safety, security, and effectiveness of such devices.

Comments are submitted by the Coalition through their counsel:

Andrew F. Sellars
Clinical Fellow, Cyberlaw Clinic
Berkman Center for Internet & Society
Harvard Law School
23 Everett Street, Second Floor
Cambridge, MA 02138
(617) 384-9125
asellars@cyber.law.harvard.edu



June 2015



United States Copyright Office

Library of Congress · 101 Independence Avenue SE · Washington, DC 20559-6000 · www.copyright.gov

June 3, 2015

Andrew Sellars
Benjamin West
Cyberlaw Clinic, Berkman Center
for Internet & Society
23 Everett Street
Second Floor
Cambridge, MA 02138

Laura Moy
New America's Open Technology
Institute
1899 L Street NW
Suite 400
Washington, D.C. 20036

Re: Docket No. 2014-7
Exemptions to Prohibition Against Circumvention of Technological
Measures Protecting Copyrighted Works

Dear Witnesses:

Thank you for your participation in the recent hearing related to Proposed Class 27—Software—networked medical devices as part of the Copyright Office's Section 1201 rulemaking proceeding. As a follow-up to certain matters discussed at the hearing, we would like to provide you with an opportunity to provide written responses to the following questions:

1. Given concerns raised by participants regarding disclosure of research results to manufacturers, please provide any additional thoughts you may have as to how the Office might approach this issue if it were to recommend the requested exemption. If some sort of disclosure to the manufacturer were required, what would that process be? Please address any relevant First Amendment or regulatory issues in your response.
2. Please briefly address how the proposed exemption might relate to or be limited by other federal or state laws or regulations, including



CYBERLAW CLINIC

Harvard Law School | Berkman Center for Internet & Society

Andrew F. Sellars
Clinical Fellow

June 29, 2015

Jacqueline C. Charlesworth
General Counsel and Associate Register of Copyrights
United States Copyright Office
Library of Congress
101 Independence Ave. SE
Washington, DC 20559-60000

**Re: Docket No. 2014-7, Exemptions to the Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works
Class 27 – Comments of Coalition of Medical Device Researchers**

Dear Ms. Charlesworth,

I write on behalf of the coalition of medical device researchers (the "Coalition")¹, in response to your letter dated June 3, 2015. The Coalition is grateful for this opportunity to respond to your questions, which are answered in turn.

A. The Copyright Office Should Not Condition an Exemption on Where Researchers Decide to Share Discoveries.

You asked the Coalition how the Copyright Office should approach the question of disclosure of research, and specifically whether and how the Copyright Office could require researchers to disclose their findings to manufacturers as a condition of the exemption. Although that is usually what happens,² there are times where the interests of safety and security are better served by disclosing research to others. Furthermore, any limitations on how and with whom researchers can discuss their work would violate the First Amendment. The Coalition therefore requests that the Copyright Office not impose any limitations on the discussion of research as a condition of the requested exemption.

As the Coalition has noted, there is no single forum for discussion of medical device security research that best ensures public safety. Today, malformed or misconfigured code in medical devices present far greater risks than exploitable vulnerabilities,³ and mandating the disclosure of information to a manufacturer first serves no greater safety purpose in those cases. Research is also often iterative, and a researcher may wish to discuss discoveries with a colleague first in

¹ The members of the Coalition are Hugo Campos, Jerome Radcliffe, Karen Sandler, and Benjamin West. *See* Coalition Comment, Appx. A.

² *See* Transcript of Hearing on Class 27 at 29–30; *see also* Coalition Reply Comment at 17–18.

³ *See* Coalition Comment at 2–3; Transcript of Hearing on Class 27 at 25.

June 2015



[Home](#) > [Academics](#) > [Clinics](#) > Samuelson-Glushko Technology Law & Policy Clinic

Samuelson-Glushko Technology Law & Policy Clinic

United States
Library of Congress

June 3, 2015

Andrew S.
Benjamin
Cyberlaw
for Intern
23 Evere
Second F
Cambrid

Laura M.
New Am
Institute
1899 L Street NW
Suite 400
Washington, D.C. 20036

Re: Docket No. 2014-7
Exemptions to Prohibition Against Circumvention
Measures Protecting Copyrighted Works

Internet & Society

Andrew F. Sellars
Clinical Fellow

June 29, 2015

Circumvention of
Protections for
Researchers

Dear Ms. Charlesworth,

I write on behalf of the coalition of medical device researchers (the "Coalition")¹, in response to your letter dated June 3, 2015. The Coalition is grateful for this opportunity to respond to your questions, which are answered below.

A. The Copyright Office's Decision to Share

You asked the Coalition whether its members, who conduct research, and specifically whether they disclose their findings to the public, what happens,² there are disclosing research to others, and can discuss their work with the Copyright Office notwithstanding the requested exemption.

As the Coalition has not received any research that best ensure devices present far greater information to a manufacturer, and the process is also often iterative, and



¹ The members of the Coalition include Benjamin West. See Coalition Comment.

² See Transcript of Hearing.

³ See Coalition Comment.

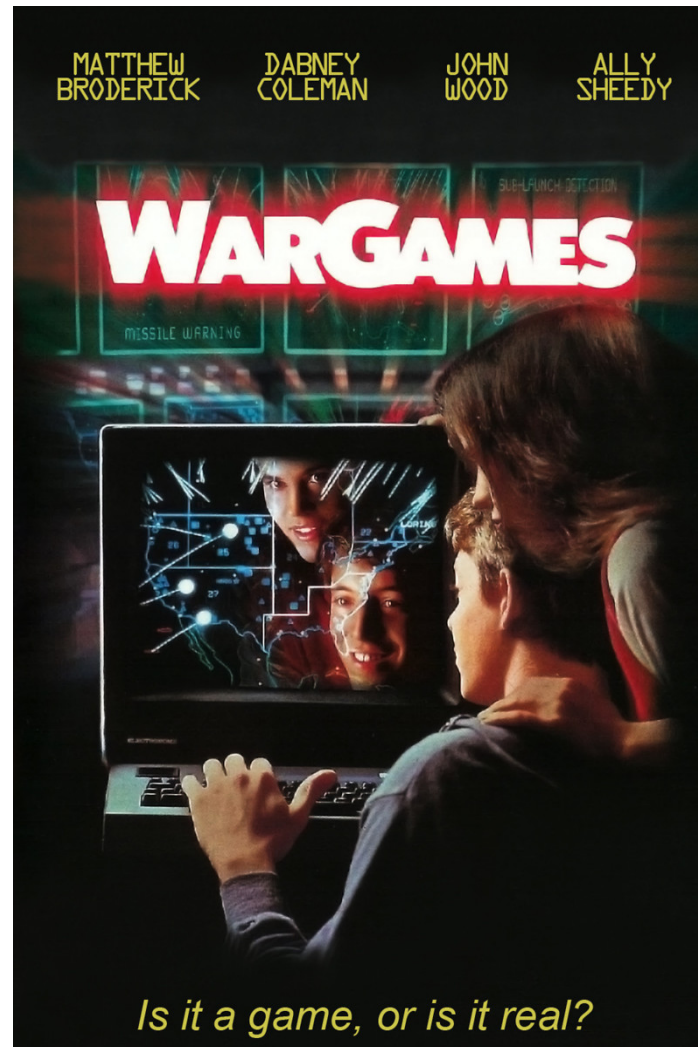
“Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research [...] and the device or machine is one of the following:”

- (A) a device or machine “designed for use by individual consumers” (including voting machines)
- (B) a “motorized land vehicle”
- (C) “A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system,” so long as the device won’t later be used in a patient

“Anticircumvention” – the law around
accessing encrypted software / media

The CFAA – the law around accessing another's computer

ROOTS OF THE CFAA



LET'S CRACK DOWN ON HACKERS

Fred Benner

(1) Sitting in front of his home computer console, a teenage boy feverishly types in password after password in an attempt to access the mystery computer he has stumbled upon. Although he is somewhat discouraged by his vain attempts to solve this particular Rubik's cube, he finally cracks the code and he is "in." Like a kid in a candy store, he excitedly applies his small amount of knowledge of computers obtained through a summer course and "browses" through the system. After a thorough look, he hangs up the phone, finishes his algebra homework, and goes to bed, satisfied with his computer safecracking achievement.

(2) Does this sound like a scene from the popular movie, War Games? As impossible as it seems, our mental image of the computer "hacker" (so-named for the ability to hack-up computer systems) is not so far from reality, but not as glamorous as it looks. Hacking should be recognized as nothing more than what it really is--breaking and entering, invasion of privacy, and in some cases, theft and destruction of property. It should also show why there is a need for government regulation of home computers.



LET'S CRACK DOWN ON HACKERS

Fred Benner

(1) Sitting in front of his home computer console, a teenage boy feverishly types in password after password in an attempt to access the mystery computer he has stumbled upon. Although he is somewhat discouraged by his vain attempts to solve this particular Rubik's cube, he finally cracks the code and he is "in." Like a kid in a candy store, he excitedly applies his small amount of knowledge of computers obtained through a summer course and "browses" through the system. After a thorough look, he hangs up the phone, finishes his algebra homework, and goes to bed, satisfied with his computer safecracking achievement.

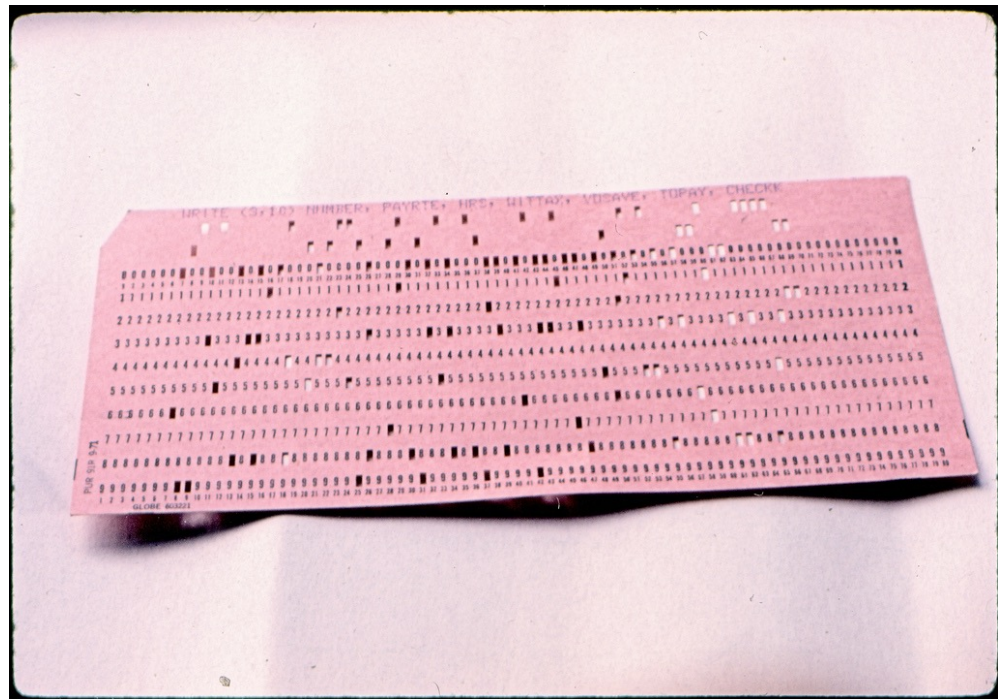
(2) Does this sound like a scene from the popular movie, War Games? As impossible as it seems, our mental image of the computer "hacker" (so-named for the ability to ~~hack up computer systems~~) is not so far from reality, but not as glamorous as it looks. Hacking should be recognized as nothing more than what it really is--breaking and entering, invasion of privacy, and in some cases, theft and destruction of property. It should also show why there is a need for government regulation of home computers.



ROOTS OF THE CFAA

1970s – 80s

- “trespass”
- “fraud”
- “property”



THE CFAA TODAY

18 U.S.C. § 1030(a)

- (1) access a computer without authorization or exceeding authorized access, and obtain classified or atomic energy information, with reason to believe that information could be used to injure the United States
- (2) access a computer without authorization or exceeding authorized access, and obtain “information from any protected computer”
- (3) access without authorization any nonpublic computer of an agency of the United States government
- (4) with intent to defraud, access a computer without authorization or exceeding authorized access, and by doing so further the intended fraud and obtain a thing of value



THE CFAA TODAY

18 U.S.C. § 1030(a)

- (5) (A) knowingly cause transmission of a program, and intentionally cause damage
 - (B) intentionally access computer without authorization, and as a result, recklessly cause damage
 - (C) intentionally access a computer without authorization, and as a result cause damage and loss
- (6) trafficking in passwords through which a computer may be accessed without authorization
- (7) with an intent to extort, transmit a threat to cause damage to a computer or obtain information from a computer without authorization



THE CFAA TODAY

Putting them together

- (1) the obtaining classified / atomic energy information one
- (2) the “obtaining information” one
- (3) the access to nonpublic fed. computers one
- (4) the “fraud, but with computers” one
- (5) the three “damage” crimes
- (6) password trafficking
- (7) the “extortion, but with computers” one

THE CFAA TODAY

Putting them together

(1) the obtaining classified / atomic energy information one

(2) the “obtaining information” one

(3) the access to nonpublic fed. computers one

(4) the “fraud, but with computers” one

(5) the three “damage” crimes

(6) password trafficking

(7) the “extortion, but with computers” one

(a) Whoever–

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains [...] (C) information from any protected computer

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [not counting use of the computer, if that use is not worth more than \$5000]

(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss

shall be punished as provided[.]

(a) Whoever–

(2) intentionally accesses a computer **without authorization or exceeds authorized access**, and thereby obtains [...] (C) information from any protected computer

(4) knowingly and with intent to defraud, accesses a protected computer **without authorization, or exceeds authorized access**, and by means of such conduct furthers the intended fraud and obtains anything of value [not counting use of the computer, if that use is not worth more than \$5000]

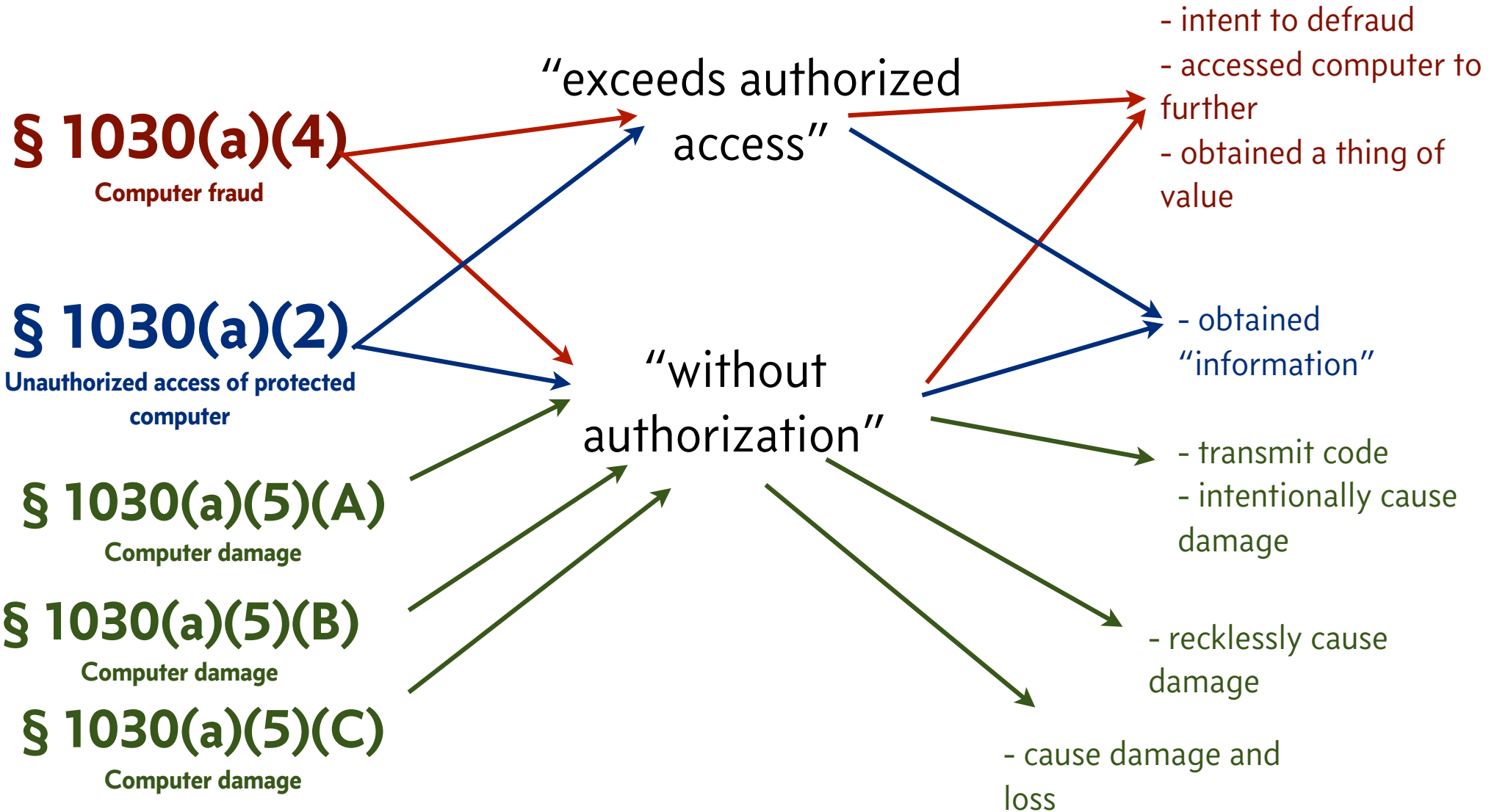
(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage **without authorization**, to a protected computer;

(B) intentionally accesses a protected computer **without authorization**, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer **without authorization**, and as a result of such conduct, causes damage and loss

shall be punished as provided[.]

CFAA CLAIMS



CFAA CLAIMS

§ 1030(a)(4)

Computer fraud

“exceeds authorized access”

- intent to defraud
- accessed computer to further
- obtained a thing of value

the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

§ 1030(a)(5)(B)

Computer damage

- recklessly cause damage

§ 1030(a)(5)(C)

Computer damage

- cause damage and loss



CEAA CLAIMS

Morris also contends that the District Court should have instructed the jury on his theory that he was only exceeding authorized access. The District Court decided that it was unnecessary to provide the jury with a definition of “authorization.” We agree. Since the word is of common usage, without any technical or ambiguous meaning, the Court was not obliged to instruct the jury on its meaning. *See, e.g., United States v. Chenault*, 844 F.2d 1124, 1131 (5th Cir.1988) (“A trial court need not define specific statutory terms unless they are outside the common understanding of a juror or are so technical or specific as to require a definition.”).

§ 1030(a)(4)
Computer fraud

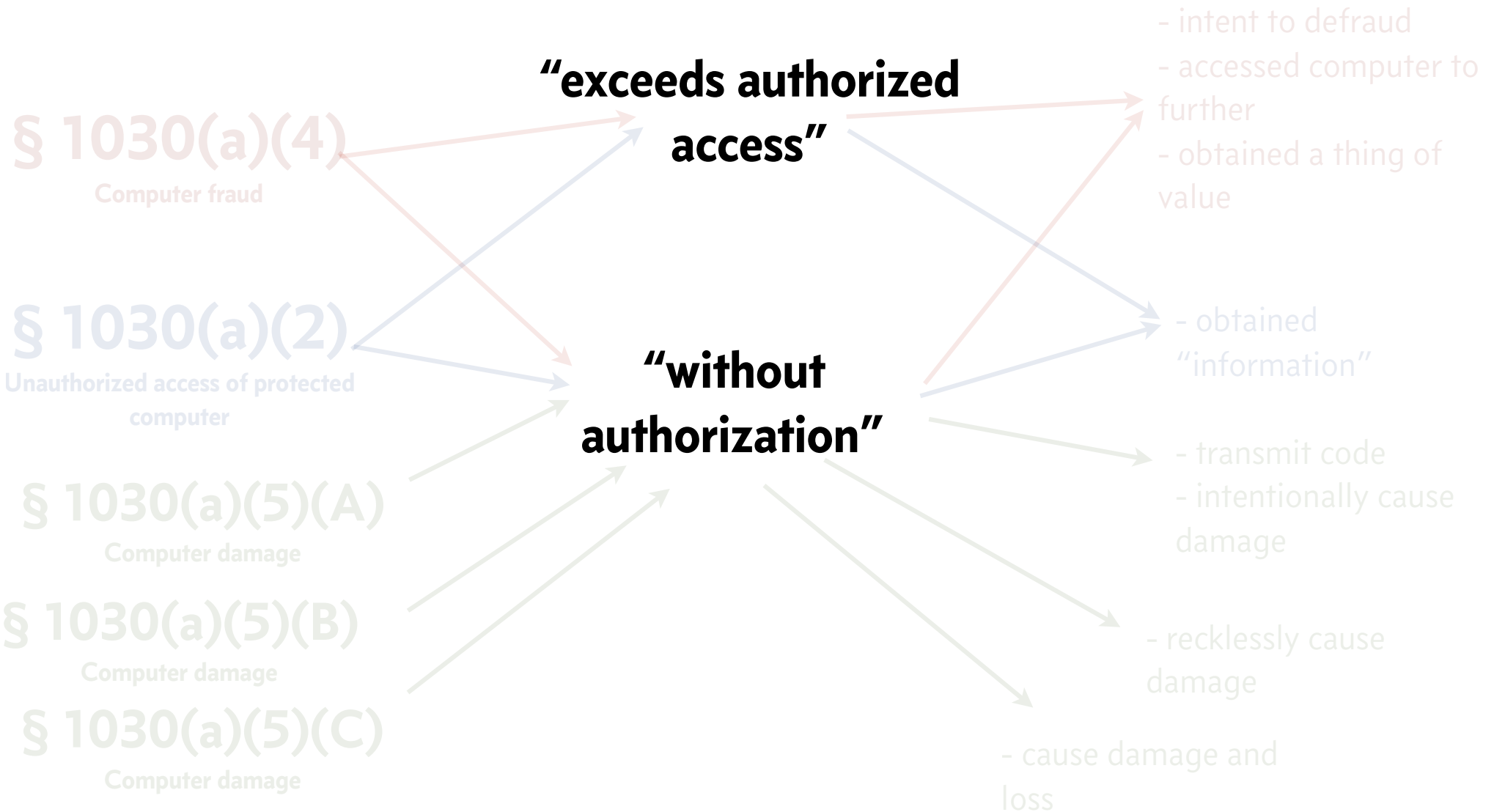
§ 1030(a)(2)
Unauthorized access of protected computer

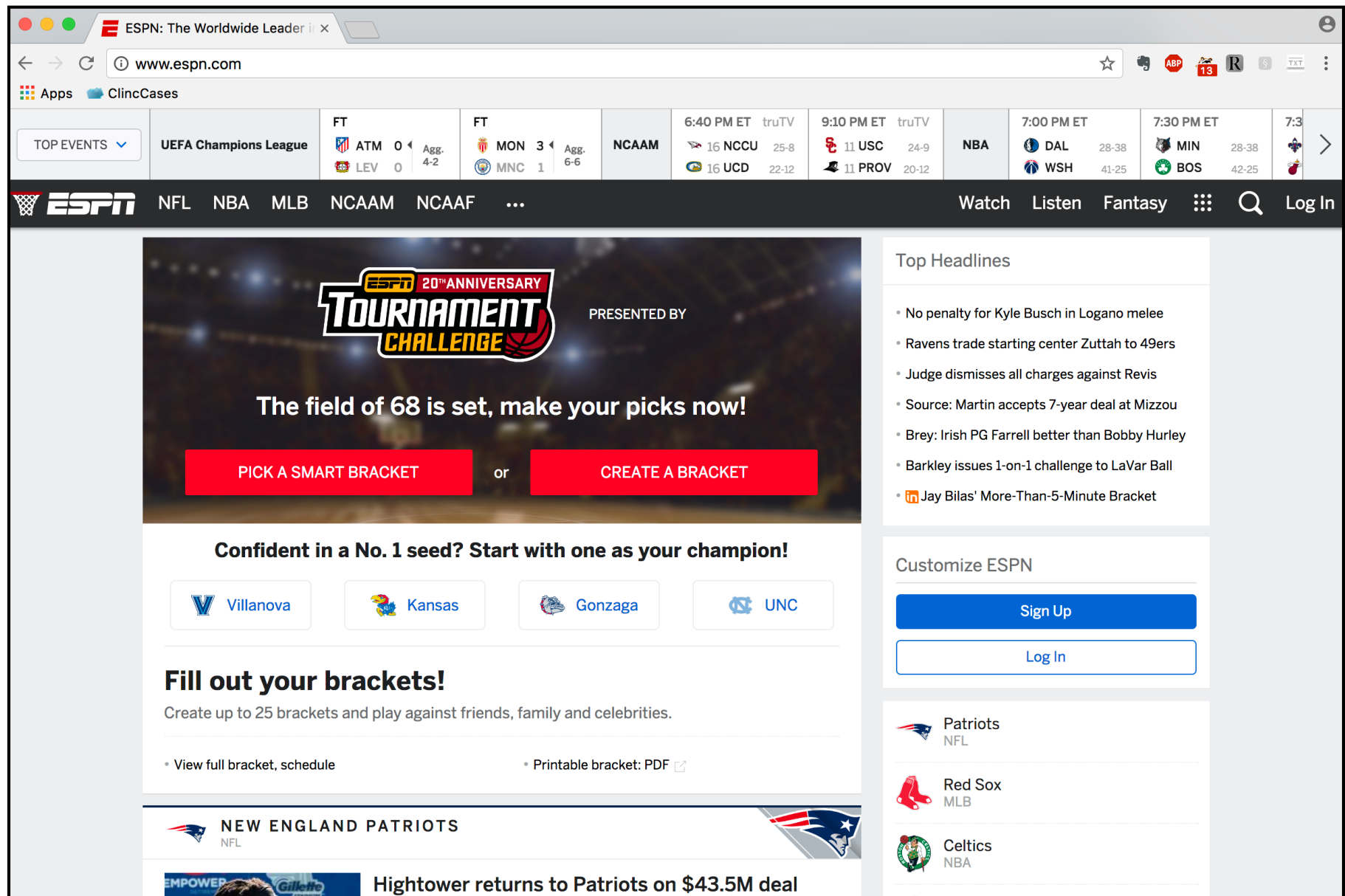
§ 1030(a)(5)
Computer damage

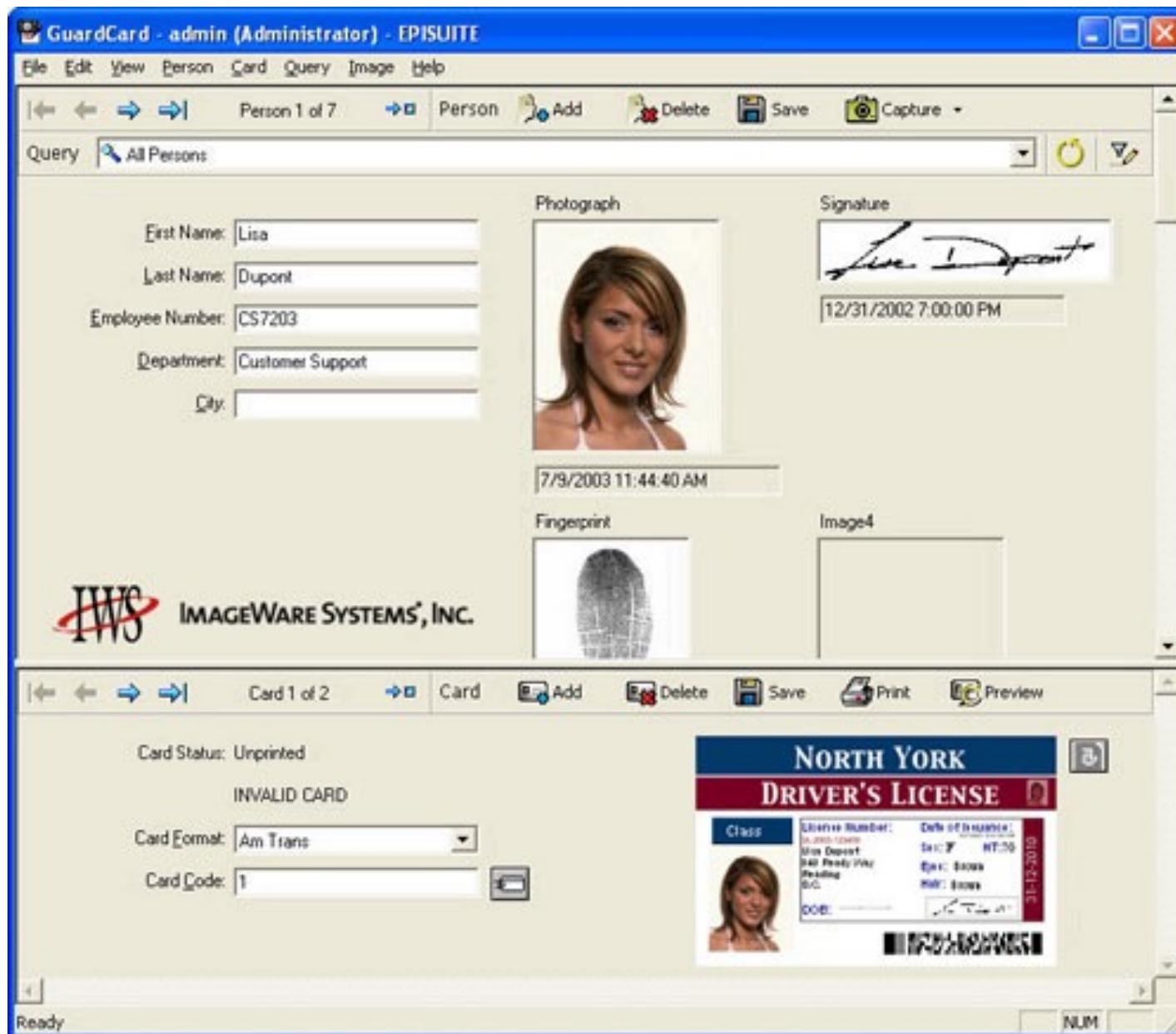
§ 1030(a)(5)(1)
Computer damage

§ 1030(a)(5)(2)
Computer damage

CFAA CLAIMS









Measuring Computer Use Norms

Matthew B. Kugler*

ABSTRACT

Unauthorized use of computer systems is at the core of computer trespass statutes, but there is little understanding of where everyday people draw the line between permissible and impermissible computer use. This Article presents a study that measures lay authorization beliefs and punishment preferences for a variety of computer misuse activities. Though perceived authorization is strongly predictive of punishment preferences, many people view common misuse activities as unauthorized but not deserving of any meaningful punishment. Majorities also viewed as unauthorized many activities—such as ignoring a website’s terms of service, surfing the news while at work, or connecting to a neighbor’s unsecured wireless network—that scholars have argued are implicitly licensed. This divergence between perceived authorization and desired punishment presents a challenge for the trespass framework.

TABLE OF CONTENTS

INTRODUCTION	1568
I. THE ROLE OF SOCIAL NORMS IN COMPUTER USE AND STUDY DESIGN.....	1570
A. <i>Participants, Procedure, and Measures</i>	1571
B. <i>Overall Relationships Between Authorization, Blameworthiness, and Punishment</i>	1573
II. MISUSE OF AN EMPLOYER’S COMPUTER	1574
III. ACCESSING A NEIGHBOR’S WI-FI NETWORK	1581
IV. ACCESSING A BUSINESS’S WEBSITE	1584
CONCLUSION	1588



Measuring Computer Use Norms

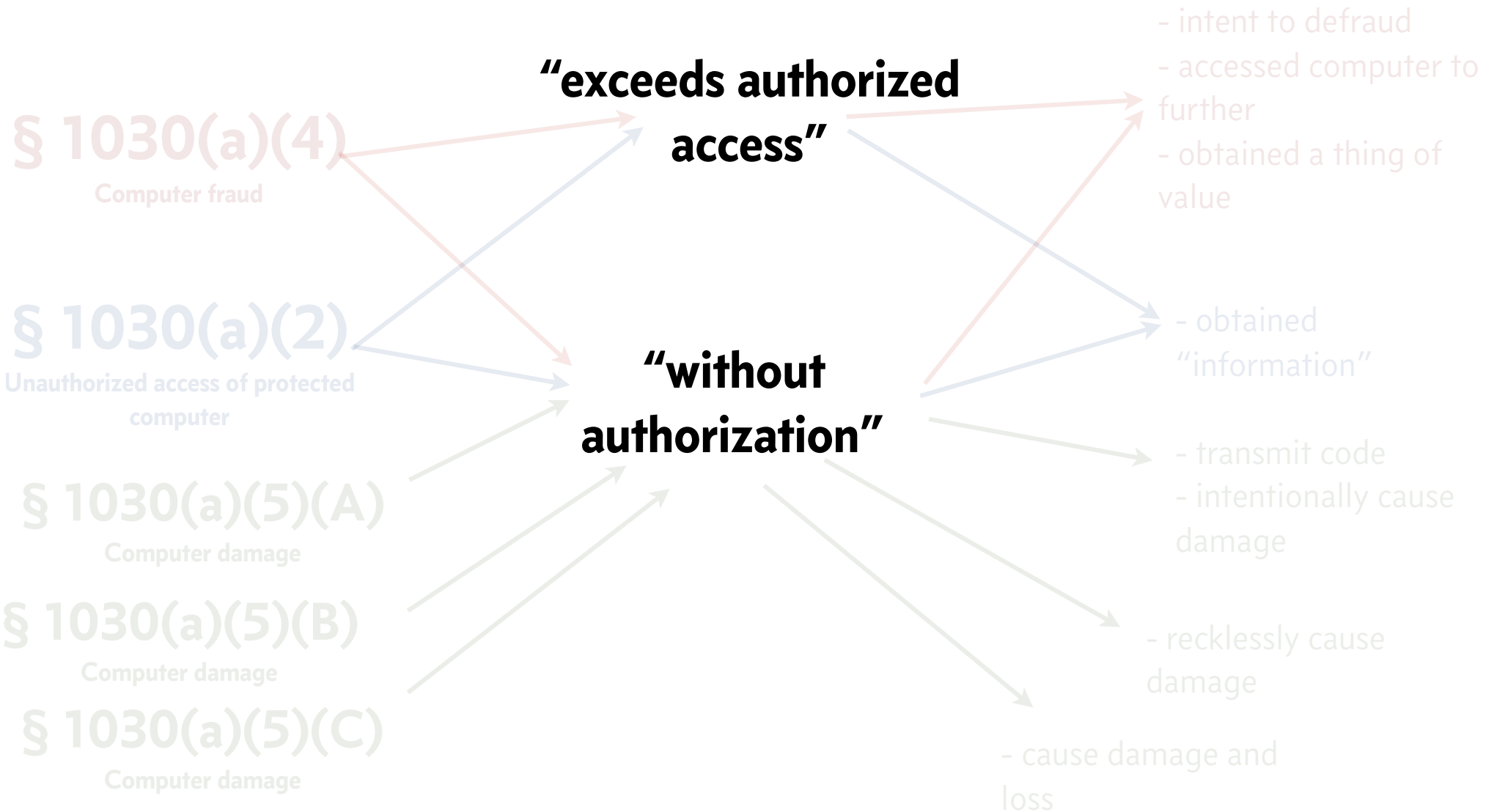
TABLE 2. ATTITUDES TOWARD USING AN EMPLOYER'S COMPUTER FOR VARIOUS NONWORK PURPOSES

	<i>Checking Weather and News</i>	<i>Examining Files of Neighbors</i>	<i>Selling Trade Secrets</i>
Authorized	2.32 (1.60)	1.44 (1.17)	1.43 (1.23)
Blameworthy	3.37 (1.64)	5.21 (1.46)	5.40 (1.40)
Punishment	1.51 (0.70)	3.08 (0.93)	3.65 (0.74)
- No Punishment	59.5%	7.6%	3.8%
- Parking Ticket	31.6%	16.5%	4.8%
- Petty Theft	7.6%	36.8%	14.4%
- Burglary	1.4%	39.2%	77.0%

III. ACCESSING A NEIGHBOR'S WI-FI NETWORK	1581
IV. ACCESSING A BUSINESS'S WEBSITE	1584
CONCLUSION	1588



CFAA CLAIMS





“Guys I got a weird Twitter DM from [W]ikileaks. See below. I tried the password and it works and the about section they reference contains the next pic in terms of who is behind it. Not sure if this is anything but it seems like it’s really wikileaks asking me as I follow them and it is a DM. Do you know the people mentioned and what the conspiracy they are looking for could be? These are just screen shots but it’s a bully built out page claiming to be a PAC let me know your thoughts and if we want to look into it.”⁹⁸



