

Legal Tactics in Cybersecurity Research

Andy Sellars
BU/MIT Technology Law Clinic
Boston University School of Law

Legal Services for Student Research and Creation

MIT and BU Students: [Click Here for Our Intake Questionnaire](#)

The BU/MIT Technology Law 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 TLC is part of the BU/MIT Entrepreneurship, Intellectual Property & Cyberlaw Program, a collaboration between Boston University School of Law and the Massachusetts Institute of Technology. Along with its companion clinic — the [Startup Law 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. The clinic is also a member of the [Free Expression Legal Network](#).

Currently-enrolled MIT and BU students who would like to speak with the clinic can fill out an [intake questionnaire](#). Don't be afraid to reach out! Sometimes your innovations need a little TLC.

Legal Services for Student Research and Creation

MIT and BU Students: [Click Here for Our Intake Questionnaire](#)

The BU/MIT Technology Law 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 TLC is part of the BU/MIT Entrepreneurship, Intellectual Property & Cyberlaw Program, a collaboration between Boston University School of Law and the Massachusetts Institute of Technology. Along with its companion clinic — the [Startup Law 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. The clinic is also a member of the [Free Expression Legal Network](#).

Currently-enrolled MIT and BU students who would like to speak with the clinic can fill out an [intake questionnaire](#). Don't be afraid to reach out! Sometimes your innovations need a little TLC.

- sites.bu.edu/techlaw
- techlaw@bu.edu
- sellars@{bu.edu, mit.edu}

Cybersecurity Research: Addressing the Legal Barriers and Disincentives

Report of a Workshop convened by
the Berkeley Center for Law & Technology,
the UC Berkeley School of Information
and the International Computer Science Institute
under a grant from the National Science Foundation
Award No. #1541881

NSF Program Solicitation: 14-599, Secure and Trustworthy Cyberpace (SaTC)¹

Background

It is blindingly clear that corporate, govt or attack. These vulnerabilities expose corporate secrets, and personal safety) improve the security of these systems. However, inquiry into vulnerabilities is under multiple U.S. laws and is further self and legal restrictions that are in a that their work could put them or their institutions are concerned with potential exposures such as former employees even concerns about work that reads too cl

¹The workshop was supported by Nemes drafted by Dennis Metzger, Nick Dwyer, a Vani Pavani, and Joseph L. Reizenstein (all).

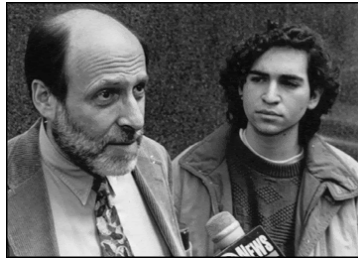
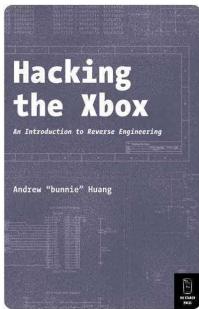
²See, for example, Elizabeth A. Hines, *NI* *Info. Rights Commission* "Advises," *New York University Law Review* (2013).

³See, for example, Michael Riley and Just English *Advises*, "Researching Business, but rights and destruction that could provide aggregated with data from the APF and a defense and intelligence officials and Gov. July 20, 2013 (reporting law of 21, 1 million dollars).

⁴Andy Greenberg, "Hackers Remotely Hijacking an researcher's ability to reveal information given's will connect).


tinkering and modification. While there are arguments that the laws at issue would not be used to actually prosecute legitimate cybersecurity research, the laws are ambiguous and can be broadly interpreted, generating uncertainty that has a wide chilling effect.

The chilling effect of these barriers takes many forms: Academic and other research institutions can be risk-averse, advising faculty and students to steer clear of research with unclear liability; faculty may advise students to work in areas less fraught with potential legal and public-relations challenges; and peer review may look unfavorably upon researchers whose work treads too closely to legal lines.¹⁹ Funders may be reluctant to support certain kinds of research. Academic publication venues are forced to wrestle with questions regarding the legality of research, despite its public value. Papers have been both delayed and outright pulled due to court intervention, threats of suit by research subjects, and program committee concerns with potential liability exposure for the committee, the institution, or the venue.²⁰ Independent researchers face an outsized threat of criminal prosecution and civil litigation. Researchers at corporations face a chill as well, because the questionable legality of certain security research may raise an appearance of impropriety if another company's technology is the subject of analysis.



Monetize without ads.
Let your visitors help you mine Bitcoins.

[Learn more](#) [Sign up](#)



6.857: Computer and Network Security



```

EC901 0402AC9D 000000005B8 00C8
const ticket # ticket type value
      (in cents)
-----
0150342 248 A84EBD 132 BE 1
time const time last last const
reader station (approx)
used used
028 0002 000000002025D0000 FD60
last trans # of const checksum
(in nickels) uses (approx)
  
```

Data layout of the CharlieCard.

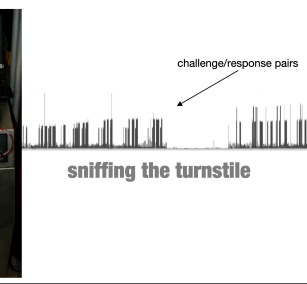
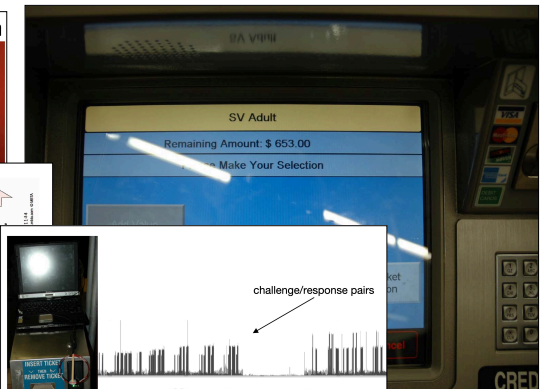
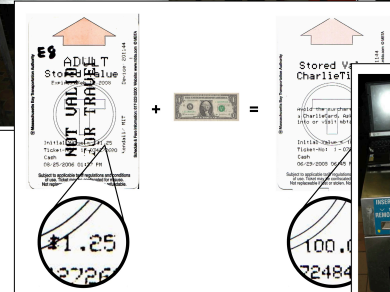
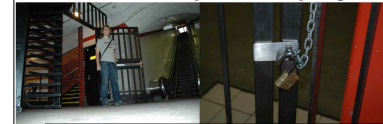
DEFCON 16

The Anatomy of a Subway Hack: Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson Student, MIT
RJ Ryan Student, MIT
Alessandro Chessa Student, MIT

Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

there is almost always a free way to get in



what this talk is not:

evidence in court
(hopefully)

what this talk is not:

evidence in court
(hopefully)

3

UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY
TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN,
ALESSANDRO CHIESA, and the
MASSACHUSETTS INSTITUTE OF
TECHNOLOGY

Defendants

Civil Action No. _____

08 CA 11364 GAO
RBC

COMPLAINT

Legal Services for Student Research and Creation

MIT and BU Students: [Click Here for Our Intake Questionnaire](#)

The BU/MIT Technology Law 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 TLC is part of the BU/MIT Entrepreneurship, Intellectual Property & Cyberlaw Program, a collaboration between Boston University School of Law and the Massachusetts Institute of Technology. Along with its companion clinic – the [Startup Law 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. The clinic is also a member of the [Free Expression Legal Network](#).

Currently-enrolled MIT and BU students who would like to speak with the clinic can fill out an [intake questionnaire](#). Don't be afraid to reach out! Sometimes your innovations need a little TLC.





The Computer Fraud and Abuse Act



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.

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 "espionage, but with computers" 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 "espionage, but with computers" 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

§ 1030(a)(4)
Computer fraud

“exceeds authorized
access”

- intent to defraud
- accessed computer to further fraud
- obtained a thing of value (except use of computer, usually)

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

access
“without
authorization”

- obtained “information”
- Protected computer

§ 1030(a)(5)(B)
Computer damage

- Cause damage (recklessly)

§ 1030(a)(5)(C)
Computer damage

- cause damage
- cause loss

§ 1030(a)(5)(A)
Computer damage

- transmit code
- intentionally cause damage “without authorization”

CFAA CLAIMS

§ 1030(a)(4)
Computer fraud

“exceeds authorized
access”

- intent to defraud
- accessed computer to further fraud
- obtained a thing of value (except use of computer, usually)

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

- obtained “information”
- Protected computer

§ 1030(a)(5)(B)
Computer damage

- Cause damage (recklessly)

§ 1030(a)(5)(C)
Computer damage

- cause damage
- cause loss

§ 1030(a)(5)(A)
Computer damage

- transmit code
- intentionally cause damage “without authorization”

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;



(e) As used in this section —

(6) 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 accessor is **not entitled so to obtain** or alter;

(e) As used in this section —

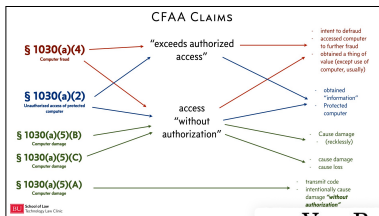
(6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is **not entitled so to obtain** or alter;

Van Buren: “in the same manner”

Gov’t: “under the same circumstances”

(e)

Van Buren’s account of “so”—namely, that “so” references the previously stated “manner or circumstance” in the text of §1030(e)(6) itself—is more plausible than the Government’s. “So” is not a free-floating term that provides a hook for any limitation stated anywhere. It refers to a stated, identifiable proposition from the “preceding” text; indeed, “so” typically “[r]epresent[s]” a “word or phrase already employed,” thereby avoiding the need for repetition. 15 Oxford English Dictionary, at 887; see Webster’s Third New International Dictionary 2160 (1986) (so “often used as a substitute . . . to express the idea of a preceding phrase”). Myriad



Van Buren’s account of subsection (a)(2) makes sense of the statutory structure because it treats the “without authorization” and “exceeds authorized access” clauses consistently. Under Van Buren’s reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.⁸ And

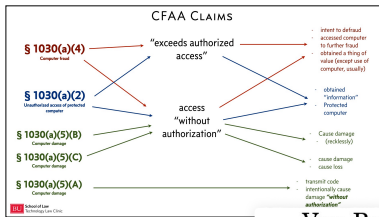
reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry. See *supra*, at 11–12.⁹

(e) As used in this section

(6) the term “exceeds a with authorization and t in the computer that the

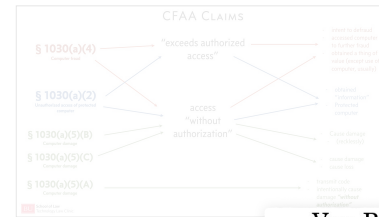
That reading, moreover, is perfectly consistent with the way that an “appropriately informed” speaker of the language would understand the meaning of “exceeds authorized access.” Nelson, *What Is Textualism?* 91 Va. L. Rev. 347, 354 (2005). When interpreting statutes, courts take note of terms that carry “technical meaning[s].” A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* 73 (2012). “Access” is one such term, long carrying a “well established” meaning in the “computational sense”—a meaning that matters when interpreting a statute about computers. American Heritage Dictionary 10 (3d ed. 1992). In the computing context, “access” references the act of entering a computer “system itself” or a particular “part of a

computer system,” such as files, folders, or databases.⁶ It is thus consistent with that meaning to equate “exceed[ing] authorized access” with the act of entering a part of the system to which a computer user lacks access privileges.⁷ The Government and the dissent’s broader interpretation is neither the only possible nor even necessarily the most natural one.



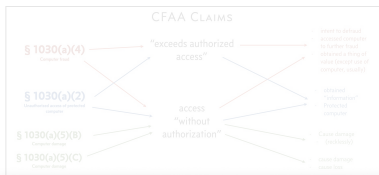
Van Buren’s account of subsection (a)(2) makes sense of the statutory structure because it treats the “without authorization” and “exceeds authorized access” clauses consistently. Under Van Buren’s reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.⁸ And

reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry. See *supra*, at 11–12.⁹



Van Buren’s account of subsection (a)(2) makes sense of the statutory structure because it treats the “without authorization” and “exceeds authorized access” clauses consistently. Under Van Buren’s reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.⁸ And

reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry. See *supra*, at 11–12.⁹



⁸ For present purposes, we need not address whether this inquiry turns only on technological (or “code-based”) limitations on access, or instead also looks to limits contained in contracts or policies. Cf. Brief for Orin Kerr as *Amicus Curiae* 7 (urging adoption of code-based approach).

can or cannot access a computer system, and one either can or cannot access certain areas within the system.⁸ And reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry. See *supra*, at 11–12.⁹

CFAA CLAIMS

§ 1030(a)(4)
Computer fraud

“exceeds authorized access”

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 accessor is not entitled so to obtain or alter;

intent to defraud
accessed computer
to further fraud
obtained a thing of
value (except use of
computer, usually)

§ 1030(a)
Unauthorized access of
computer

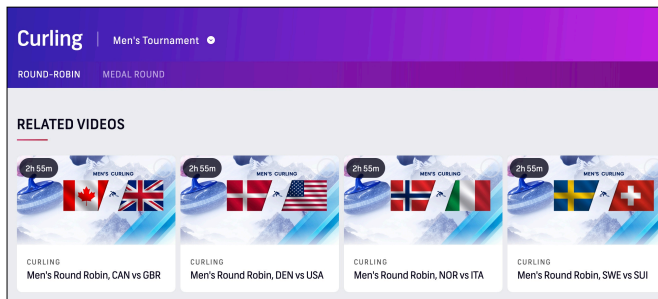
obtained
“information”
Protected
computer

Per *Van Buren v. United States* (2021)...

- “so” in “not entitled so to obtain” means “in the same manner”
- should be geared towards “inside hackers” as a “gates-up-or-down” inquiry
- and when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.

“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

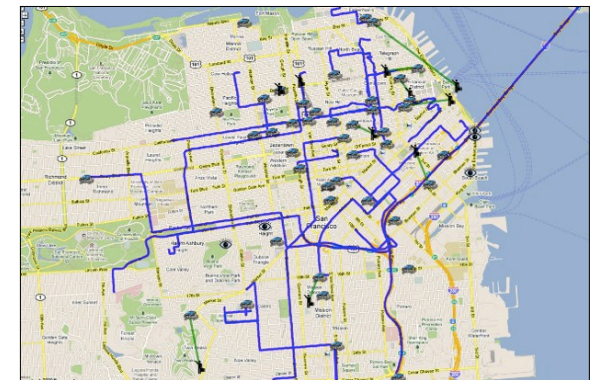
- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.



password regardless of whether you were the one performing those actions.
3. You must use the University’s computing facilities only for the University-related purposes for which they were authorized. As with all University equipment, use of the computing facilities, including the Campus Network, for private or commercial purposes is prohibited, except as expressly authorized. You must not use the University’s computing facilities for any unlawful purpose, including but not limited to the collection, installation or distribution of fraudulently or illegally obtained media files or software. Use of external networks or services – including cloud services – must comply with the policies of acceptable use published both by the University and by the organizations providing those networks or services.
4. You must not access, alter, copy, move or remove information, proprietary software or other

“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

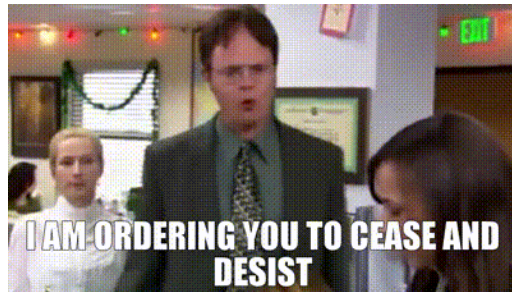
- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.



“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

```
import requests, bs4
page = requests.get('http://sites.bu.edu/techlaw/blog')
page.raise_for_status()
pageSource = bs4.BeautifulSoup(page.text, 'lxml')
titles = pageSource.select('article h2')
for i in titles:
    print(i.getText())
```

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.



“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.

“A PAC run anti-Trump site putintrump.org is about to launch. The PAC is a recycled pro-Iraq war PAC. We have guessed the password. It is 'putintrump.' See 'About' for who is behind it. Any comments?”

“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 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

BuzzFeed News
REPORTING TO YOU

SIGN IN ABOUT US GOT A TIP? SUPPORT US BUZZFEED.COM

THE MUELLER MEMOS

A New Version Of The Mueller Report Reveals That Mueller Declined To Charge Donald Trump Jr. And Roger Stone With Computer Crimes

The document was released in response to a Freedom of Information Act lawsuit filed by BuzzFeed News.

by Jason Leopold
BuzzFeed News Reporter

by Anthony Cormier
BuzzFeed News Reporter

Posted on February 11, 2022, 4:07 pm

View 49 comments

technical meanings

- but SCOTUS is not saying this has to be “code based,” at least for now.

BU School of Law
Technology Law Clinic

is about to launch. The PAC is
ed the password. It is

2. Potential Section 1030 Violation By Donald Trump Jr.

The Office also considered whether Donald Trump Jr. intentionally accessed a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(2)(C) & (c)(2)(A) (providing penalties for “[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer”). The conduct at issue was Trump Jr.’s use of a password, supplied to him by WikiLeaks in a Twitter direct message, to access the website “putintrump.org” in September 2016. See Volume I, Section III.D.1.e, *supra*.

The facts known to the Office likely sufficed to establish each element of a misdemeanor violation of Section 1030(a)(2)(C). Trump Jr. received the password from WikiLeaks and then wrote to others that “it worked” when he tried it; that evidence would support a conclusion that he “accesse[d] a computer without authorization.” See *United States v. Phillips*, 477 F.3d 215, 219-220 (5th Cir. 2007) (collecting cases holding that use of a guessed password, or one belonging to a third party, constitutes unauthorized access). That same course of conduct, and Trump Jr.’s email admissions afterwards, also suggested that Trump Jr. acted “intentionally.” See *United States v.*

trigger felony punishment under the statute. See 18 U.S.C. § 1030(c)(2)(B). Given that Trump Jr. did not himself initiate the plan to access the website or guess the password, the absence of evidence that his acts caused any damage to the website or obtained valuable information, the technical nature of the violation, and the minimal punishment that a misdemeanor conviction could be expected to carry in these circumstances, the Office decided against pursuing charges.

“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.

BU School of Law
Technology Law Clinic

https://dcp2.att.com/OPENDClient/openPage?ICCID=8991101200003204510

The Markup

Prediction: Bias

Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them

“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- *but* SCOTUS is not saying this has to be “code based,” at least for now.

The company that makes it sent more than 5.9 million of these crime predictions to law enforcement agencies across the country—from California to Florida, Texas to New Jersey—and we found those reports on an unsecured server.

The Markup

Big Tech Is Watching You. We're Watching Big Tech.

Privacy

Family Safety App Touting Digital Security Leaves Its Own Users' Sensitive Data at Risk

Former employees said Life360 executives knew about security gaps
By Alfred Ng and Jon Keegan
February 17, 2022 08:00 ET

“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- *but* SCOTUS is not saying this has to be “code based,” at least for now.

What We Found

A lack of multifactor authentication

No log-in attempt limits

Lack of password change notifications

Why This Matters

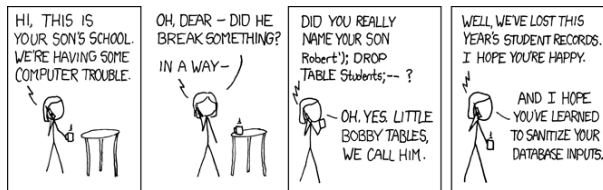
Multifactor authentication prevents an attacker from being able to log in to your accounts by having just your password alone. It usually requires a second authentication method, which can be a temporary code from a text message or an authentication app, or a physical token like a USB security key.

Attempt limits prevent attackers from making an infinite amount of guesses until they correctly guess your password. Hackers will often use bots to do this and can eventually crack most passwords without attempt limits. We were able to try the wrong password 500 times with no warning (after checking an initial checkbox labeled “I am human”).

Password change notifications warn users when their credentials are altered without their consent. Life360 logs out all other sessions once a password is changed, but the original owner is never notified when that happens. If the attacker changes the password before the real user does, the real user would effectively be locked out of their own accounts.

“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

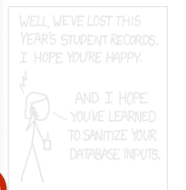
- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- *but* SCOTUS is not saying this has to be “code based,” at least for now.



“access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”

- “so” is “in the same manner”
- should be a “gates-up-or-down” inquiry
- when Congress uses technical words courts should give them their technical meanings
- *but* SCOTUS is not saying this has to be “code based,” at least for now.

The evidence permitted the jury to conclude that Morris’s use of the SEND MAIL and finger demon features constituted access without authorization. While a case might arise where the use of SEND MAIL or finger demon falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris’s conduct here falls well within the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both



CFAA CLAIMS

§ 1030(a)(4)
Computer fraud

“exceeds authorized access”

intent to defraud
accessed computer
to further fraud
obtained a thing of
value (except use of
computer, usually)

§ 1030(a)
Unauthorized access of
computer

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;

obtained
“information”
Protected
computer

Per *Van Buren v. United States* (2021)...

- “so” in “not entitled so to obtain” means “in the same manner”
- should be geared towards “inside hackers” as a “gates-up-or-down” inquiry
- and when Congress uses technical words courts should give them their technical meanings
- but SCOTUS is not saying this has to be “code based,” at least for now.

(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[.]

The screenshot shows the HackerOne website. The top navigation bar includes 'FOR BUSINESS', 'FOR HACKERS', 'HACKTIVITY', 'COMPANY', and 'TRY HACKERONE'. The main headline reads 'THE MOST TRUSTED HACKER-POWERED SECURITY PLATFORM' with a sub-headline 'More Fortune 500 and Forbes Global 1,000 companies trust HackerOne to test and secure the applications they depend on to run their business.' Below this is a 'GET STARTED' button and a 'SEE HOW IT WORKS' button. A secondary headline states 'LEAD INDUSTRY INSIGHTS FROM 1,400 ORGANIZATIONS IN THE HACKER-POWERED SECURITY REPORT'. At the bottom, there is a 'Vulnerability Reporting' section with a 'Report' button and a 'Security Vulnerability Disclosure Program' section with a 'Learn More' button. The footer includes the BU School of Law Technology Law Clinic logo.

The screenshot shows the Instacart Bug Bounty Program page. The top navigation bar includes 'SOLUTIONS', 'PRODUCTS', 'PARTNERS', 'COMPANY', 'HACKERS', and 'RESOURCES'. The main heading is 'Instacart' with the URL 'http://instacart.com'. Below this are statistics: 'Reports resolved', 'Assets in scope', and 'Average bounty'. A 'Submit report' button is visible. The page lists rules for the program, including 'Additionally, while hunting for bugs, please refrain from the following activities:'. The list includes:


- Testing for DoS issues, or any kind of issue which could affect the experience of other Instacart users
- Using automated tools which generate significant traffic
- Accessing another user's data or other private information
- Attempting to social engineer or spam Instacart employees, shoppers or other users
- Submitting reports from automated tools without any verification

 The 'Out-of-Scope' section states: 'Systems or services which are not owned or maintained by Instacart, such as third-party blogs or micro-sites, are not eligible, and we can't give you permission to test against. These include (but not limited to):'

- brand.instacart.com
- careers.instacart.com and www.careers.instacart.com
- carrotstore.instacart.com and www.carrotstore.instacart.com
- corporate.instacart.com
- covidresponse.instacart.com

 The footer includes the BU School of Law Technology Law Clinic logo.

hackerone SOLUTIONS PRODUCTS PARTNERS COMPANY HACKERS RESOURCES



UPS VDP
<https://www.ups.com>

Submit report

Vulnerability Disclosure Program
 Launched on Feb 2022
 Managed by HackerOne

Reports resolved: 2 Assets in scope: 1

Policy Hacktivity Thanks Updates (0)

Disclosure Policy

- As this is a private program, please do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the organization.
- Follow HackerOne's [disclosure guidelines](#).

BU School of Law Technology Law Clinic



BU School of Law Technology Law Clinic

Home About the Clinic Practice Areas People Blog Contact Us Frequently Asked Questions

Legal Services for Student Research and Creation

MIT and BU Students: Click Here for Our Intake Questionnaire

The BU/MIT Technology Law 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 TLC is part of the BU/MIT Entrepreneurship, Intellectual Property & Cyberlaw Program, a collaboration between Boston University School of Law and the Massachusetts Institute of Technology. Along with its companion clinic – the [Startup Law 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. The clinic is also a member of the [Free Expression Legal Network](#).

Currently-enrolled MIT and BU students who would like to speak with the clinic can fill out an [intake questionnaire](#). Don't be afraid to reach out! Sometimes your innovations need a little TLC.

Boston University BU School of Law BU Today Startup Law Clinic Follow @BUTechLaw on Twitter

BU School of Law Technology Law Clinic

News & Views Job Search Events Reports & Data **INSIDE HIGHER ED** Admissions Diversity Student Voice Membership


COVID-19 **THE TOPICAL** Michigan State Professors Want Pay Cuts Restored Students on Cheating

#News #Technology

Facebook Disables NYU Research Accounts

Facebook claims the researchers' data collection methods violate its terms of service. The recent action highlights the increasingly fraught relationship between colleges and universities and the big tech companies they research.

By Emma Whitford // August 6, 2021



TRENDING STORIES

- Truths about an academic career people often don't share (opinion)
- Colleges must change to better serve multiracial students (opinion)
- Serviceers prepare for student loan payments to resume
- What Will Higher Education Look Like 15 Years From Now? | Higher Ed Gamma
- Advice for how to make courageous decisions in academe (opinion)

BU School of Law Technology Law Clinic

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. [...]

- (c) The punishment for an offense under subsection (a) or (b) of this section is—
- (4)(A) [with some exceptions,] a fine under this title, imprisonment for not more than 5 years, or both, in the case of—
- (i) an offense under subsection (a)(5)(B), [if a first offense,] if the offense caused [or would have caused] –
 - (I) loss to 1 or more persons during any 1-year period [and for criminal cases, loss affecting 1 or more protected computers] aggregating at least \$5,000 in value;
 - (II) [impairment or modification of medical technologies]
 - (III) physical injury to any person;
 - (IV) a threat to public health or safety;
 - (V) [government computers used in administration of justice, national defense, or national security]

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. [...]

- (c) The punishment for an offense under subsection (a) or (b) of this section is—
- (4)(A) [with some exceptions,] a fine under this title, imprisonment for not more than 5 years, or both, in the case of—
- (i) an offense under subsection (a)(5)(B), [if a first offense,] if the offense caused [or would have caused] –
 - (I) loss to 1 or more persons during any 1-year period [and for criminal cases, loss affecting 1 or more protected computers] aggregating at least \$5,000 in value;
 - (II) [impairment or modification of medical technologies]
 - (III) physical injury to any person;
 - (IV) a threat to public health or safety;
 - (V) [government computers used in administration of justice, national defense, or national security]

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. [...]



Dear WGBH Supporter,

We want to make you aware that we were recently notified of a cyber incident involving Blackbaud, a service provider used by WGBH and nonprofits worldwide for fundraising and donor engagement services. Blackbaud informed us that in May 2020 they discovered unauthorized activity on their network which resulted in potential unauthorized access to certain information maintained by Blackbaud. Among this information was an older data file (sent to Blackbaud prior to 2015) containing donor information to help us conduct customer relationship management.

In addition to an investigation by Blackbaud, WGBH is conducting its own investigation to determine what, if any, sensitive WGBH data was potentially impacted. This investigation has confirmed that the incident has not exposed any checking, credit card or other financial account information, Social Security numbers or email addresses, of WGBH donors. We also determined that the file we provided Blackbaud may have included basic demographic information of WGBH donors and philanthropic engagement data.

- (V) [government computers used in administration of justice, national defense, or national security]

The CERT® Guide to Coordinated Vulnerability Disclosure

Allen D. Householder
Garret Wassermann
Ari Mennon
Chris King

August 2017

SPECIAL REPORT
CMU/SEI-2017-SR-022

CERT Division

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

<http://www.sei.cmu.edu>

DEFCON 16

The Anatomy of a Subway Hack: Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zeek Anderson Student, MIT
RJ Ryan Student, MIT
Alessandro Chiesa Student, MIT

Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WIFI: WARCARTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

19 THE COURT: Just a moment. They may think that that
20 was cute at the time that they drafted that up but that's what
21 they undertook to do and they have to accept the consequences
22 of that because as far as I'm concerned if someone does end up
23 doing this, they are aiders and abettors, yet, they have
24 undertaken to provide this information.

10 THE COURT: I haven't made judgment. It's not before
11 me. I'm making a set of observations which inform my judgment
12 about whether or not somebody else has to exercise some
13 supervision over these kids.

7 approach. Sometimes we can't expect people in their early 20's
8 to have sufficient judgment or experience to avoid causing
9 those clashes of interest between something as broad and as
10 important as the First Amendment and the need to avoid actual
11 criminal conduct of which words are the constituent elements.

MIT News

MIT researchers identify security vulnerabilities in voting app

Mobile voting application could allow hackers to alter individual votes and may pose privacy issues for users.
Abby Abazorius | MIT News Office
February 13, 2020



In recent years, there has been a growing interest in using internet and mobile technology to increase access to the voting process. At the same time, computer security experts caution that paper ballots are the only secure means of voting.



PRESS MENTIONS

ELECTION 2020

Vote on Your Phone? BU School of Law Clinic Helps Expose Security Flaws in Voter App
MIT students, working with clinic, bring election app research to Homeland Security

MIT researchers say they found critical flaws in the voting app owned by Homeland Security. They used the 2020 Election 2020 app to expose security flaws in the app.

MIT News

MIT researchers identify security vulnerabilities in voting app

Mobile voting application could allow individual votes and may pose privacy issues for users.
Abby Abazorius | MIT News Office
February 13, 2020



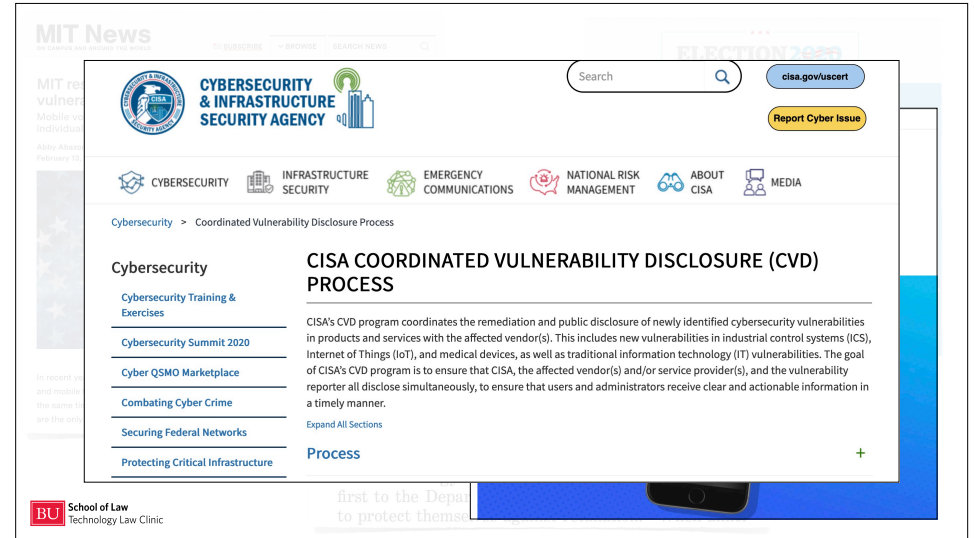
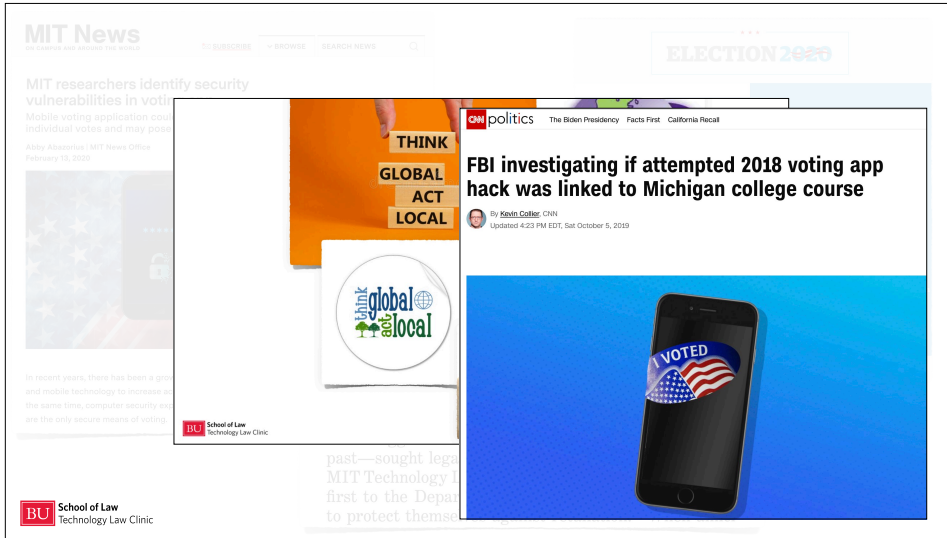
In recent years, there has been a growing interest in using internet and mobile technology to increase access to the voting process. At the same time, computer security experts caution that paper ballots are the only secure means of voting.



past—sought legal counsel from the Boston University/MIT Technology Law Clinic, and disclosed their findings first to the Department of Homeland Security, in part to protect themselves against retaliation.⁸ When amici

ELECTION 2020

Vote on Your Phone? BU School of Law Clinic Helps Expose Security Flaws in Voter App



- sites.bu.edu/techlaw
- techlaw@bu.edu
- sellers@{bu.edu, mit.edu}

