Brooklyn Law Review

Volume 87 | Issue 3 Article 8

4-19-2022

The "Worst Law in Technology": How the Computer Fraud and Abuse Act Allows Big Businesses to Collect and Sell Your Personal Information

Alicia Nakhjavan

The "Worst Law in Technology"[1]

HOW THE COMPUTER FRAUD AND ABUSE ACT ALLOWS BIG BUSINESSES TO COLLECT AND SELL YOUR PERSONAL INFORMATION

INTRODUCTION

Have you ever Googled a random product, then a few hours later logged on to Instagram and noticed an advertisement for that exact product?[2] Have you ever wished you could do something to prevent or stop these targeted ads? Targeted ads appear because of cookies[3]—small text files that keep track of your browsing information.[4] Cookies contain pieces of data, such as someone's username and password, and are used to identify a particular computer.[5] Web developers use cookies to make visiting websites more personalized and convenient for users.[6]

Often, when users visit a website for the first time, they are prompted with a message that reads "this website uses cookies in order to offer you the most relevant information."[7] For most people, it is a habit to click "accept."[8] People rarely read a website's privacy policy to learn how long these cookies will track their browsing information, or what kinds of information they track.[9] Most of the

---

[1] Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology [https://perma.cc/7ZX8-W7NS].

[2] *See* Spreeha Dutta, *How Does Instagram Show Me Ads About What I Have Searched on Google*, STARTUP (May 22, 2020), https://medium.com/swlh/how-does-instagram-show-me-posts-regarding-what-i-have-searched-on-google-20744326a4a9 [https://perma.cc/YJ4P-HEVD].

[3] *Id.*

[4] Sara Pegarella, *Cookies Notification Messages*, TERMSFEED (Dec. 22, 2020), https://www.termsfeed.com/blog/cookies-notification-messages/ [https://perma.cc/RNW6-NA26].

[5] *What Are Cookies?*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/cookies [https://perma.cc/NFC7-FNK8].

[6] *Id.*

[7] *See* Pegarella, *supra* note 4.

[8] Matthew Hughes, *Opera for Android Now Automatically Blocks Those Irritating Cookie Notifications*, NEXT WEB (Nov. 6, 2018, 8:00 AM), https://thenextweb.com/tech/2018/11/06/opera-for-android-now-automatically-blocks-those-irritating-cookie-notifications/ [https://perma.cc/4E6A-6FS2].

[9] Emily Stewart, *Why Every Website Wants You to Accept Its Cookies*, VOX (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy [https://perma.cc/Y9HS-N54E].

time, cookies do not stop tracking a user once the user leaves the website.[10] While cookies have become essential to the modern internet, their use raises serious privacy concerns about what information is collected, where it is stored, and to whom it is transmitted.[11]

The right to privacy is essential to Americans.[12] Privacy allows people to protect themselves from unwanted interference in their lives and retain control over what and how much others know about them.[13] In 1965, the US Supreme Court recognized that the right to privacy was important enough to be deemed a fundamental right.[14] Today, eleven states explicitly recognize the right to privacy in their constitutions[15] and other states have introduced privacy legislation.[16] Seventeen states have specifically introduced internet privacy laws to give consumers control over their data and how websites use it.[17] These internet privacy laws aim to address the privacy issues that both internet use and advancing technologies raise.

Technology has always been intertwined with privacy.[18] As technology advances, so does the capability to protect privacy.[19] On the other hand, advancing technology means more opportunities for large companies[20] to collect users' personal information without or in excess of their authorization.[21] Today, hundreds of companies collect personal data, such as names and addresses, about their internet users daily.[22] Most of this

---

[10] Dennis Anon, *How Cookies Track You Around the Web and How to Stop Them*, PRIVACY.NET (Feb. 24, 2018), https://privacy.net/stop-cookies-tracking/ [https://perma.cc/ZWD2-22UJ].

[11] *See What Are Cookies?*, *supra* note 5.

[12] *See What Is Privacy?*, PRIV. INT'L (Oct. 23, 2017), https://privacyinternational.org/explainer/56/what-privacy [https://perma.cc/3X22-NCF3].

[13] *Id.*

[14] *See* Griswold v. Connecticut, 381 U.S. 479, 494 (1965).

[15] Pam Greenberg, *Privacy Protections in State Constitutions*, NAT'L CONF. OF STATE LEGISLATURES (Nov. 6, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx [https://perma.cc/UFY9-GV34].

[16] Gretchen A. Ramos & Darren Abernethy, *Additional U.S. States Advance the State Privacy Legislation Trend in 2020*, NAT'L L. REV. (Jan. 27, 2020), https://www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020 [https://perma.cc/6J9U-6JSA].

[17] *Status of Internet Privacy Legislation by State*, AM. C.L. UNION (Nov. 14, 2020), https://www.aclu.org/issues/privacy-technology/internet-privacy/status-internet-privacy-legislation-state [https://perma.cc/V4F7-TRLZ].

[18] *See What Is Privacy?*, *supra* note 12.

[19] *Id.*

[20] This note uses "big businesses" and "large companies" interchangeably.

[21] *See What Is Privacy?*, *supra* note 12.

[22] Steven Melendez & Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/SD5C-QPQV].

personal data is collected through laptops or smartphones.[23] Companies then use this data to send personalized, targeted ads.[24] One example of a targeted ad is location-based advertising, which tracks and uses a person's geographic location to provide them with advertisements for nearby businesses.[25]

Businesses can track and collect far more than just information about your geographic location.[26] For example, when a person uses Facebook's camera feature, Facebook collects information about what a person sees through the camera.[27] Facebook then uses this information to suggest new photo filters that a particular user may like or give a user tips on how to use camera formats.[28] Facebook also provides this information to advertisers, measurement partners, vendors, and other third parties.[29] Some companies may even sell any collected data to other advertising companies or data brokers, profiting from users' personal information.[30] Often, people do not understand what kinds of personal information companies collect or with whom this information is shared.[31]

Although large companies have been collecting information from online users for years,[32] states are just beginning to respond to the privacy issues raised by this data collection.[33] Following the passage of the California Consumer Privacy Act (CCPA) in 2018,[34] many "states proposed similar

---

[23] Max Freedman, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY (June 17, 2020), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/V9TB-DF84].

[24] *Id.*

[25] *Complete Guide to Location-Based Advertising (LBA) in 2021—Geo-Targeting, Geo-Fencing, Geo-Conquesting, Proximity Targeting*, KNOREX, https://www.knorex.com/blog/articles/location-based-mobile-advertising#Fastfoodchains [https://perma.cc/W5QW-8B63].

[26] *See* Caitlin Dewey, *98 Personal Data Points that Facebook Uses to Target Ads to You*, WASH. POST (Aug. 19, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/ [https://perma.cc/Y2W2-8X2G].

[27] *Data Policy*, FACEBOOK (Jan. 11, 2021), https://www.facebook.com/privacy/explanation [https://perma.cc/BL8V-HQRX].

[28] *Id.*

[29] *Id.*

[30] *See* Freedman, *supra* note 23.

[31] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/28JK-ZGFQ].

[32] *Id.*

[33] *See* Mitchell Noordyke, *U.S. State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PROS. (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/ [https://perma.cc/82JU-2QE4].

[34] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020). The CCPA gives California consumers more control over the personal information businesses collect from them by establishing new privacy rights, including the right to: (1) know what "personal information a business collect[ed]" and "how it is [being]

legislation to protect consumers" from the collection of their personal data.[35] While the CCPA allows consumers whose personal information is accessed without authorization to bring a private civil action against a company that violates the law,[36] other states' proposed legislation does not permit consumers to bring private civil actions against companies.[37] This means that under most state laws, consumers are unable to sue and obtain monetary damages or injunctive relief from businesses that collect their personal information without authorization.[38]

Further, there is currently no federal law that creates a private right of action against a large company when it collects consumers' personal information without authorization.[39] The closest a federal law has come to providing this type of remedy is through the Computer Fraud and Abuse Act of 1986 (CFAA).[40] Under the CFAA, any person may bring a private civil action where the defendant accessed a protected computer without or in excess of authorization if the offense caused one of the kinds of loss specified by the statute.[41] Congress has acknowledged that significant gaps in the CFAA will emerge as technology advances.[42] To close these gaps and fulfill the CFAA's purpose of being a comprehensive law to address computer crimes, Congress has repeatedly amended the CFAA.[43] The CFAA was amended in 1994, 2001, and 2008.[44] Since

---

used and shared"; (2) "delete personal information collected from them"; (3) "opt-out of the sale of . . . personal information"; and (4) "non-discrimination for exercising . . . CCPA rights." *California Consumer Privacy Act (CCPA)*, CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/JRF5-AAK3].

[35] *See* Noordyke, *supra* note 33.

[36] David O. Klein, *United States: CCPA Law: The Private Right of* Action, MONDAQ (Feb. 28, 2020), https://www.mondaq.com/unitedstates/privacy-protection/898694/ccpa-law-the-private-right-of-action [https://perma.cc/H63N-UFK7]. Under the CCPA, a California consumer can only bring a civil right of action against a business if that business fails to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." *Id.*

[37] *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Apr. 2, 2021), https://www.varonis.com/blog/us-privacy-laws/ [https://perma.cc/38QU-MRG4].

[38] *See id.*

[39] *See* BECKY CHAO ET AL., NEW AM., ENFORCING A NEW PRIVACY LAW: WHO SHOULD HOLD COMPANIES ACCOUNTABLE? 16 (Nov. 20, 2019), https://bit.ly/3DP81k1 [https://perma.cc/UE3C-ZPQJ] (see section entitled "A Private Right of Action is Key to Ensuring that Consumers Have Their Own Avenue for Redress").

[40] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (amending 18 U.S.C. § 1030).

[41] 18 U.S.C. § 1030(g).

[42] S. REP. NO. 104-357, at 5 (1996).

[43] *CFAA Background*, NAT'L ASS'N OF CRIM. DEF. LAWS. (Mar. 10, 2020), https://www.nacdl.org/Content/CFAABackground [https://perma.cc/L2NW-NSMH].

[44] *Id.* While the CFAA was also amended in 1988, 1989, 1990, 1996, and 2002, this note only focuses on the 1994, 2001, and 2008 amendments. COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES 2 (2017) [hereinafter PROSECUTING COMPUTER CRIMES], https://www.justice.gov/criminal/file/442156/download [https://perma.cc/U66M-N89F].

its last amendment in 2008, technology has advanced beyond what Congress could have then imagined,[45] changing how people work, live, and entertain themselves.[46] These advances in technology, and our dependence on it, have created new gaps in the CFAA.[47]

To bring a civil claim under the CFAA, the offense must have caused a loss of at least $5,000 to one or more persons.[48] If this $5,000 minimum is not met, the claim will be dismissed for lack of jurisdiction.[49] The CFAA's definition of loss is very narrow and is limited to "technological harms to computer data or systems."[50] Specifically, this definition does not cover personal information, such as name, gender, zip code, phone activity, geological data, or other unique identifiers.[51] Many people have brought lawsuits against big companies claiming a loss of personal privacy and alleging that the company collected or used their personal information without or in excess of authorization in violation of the CFAA.[52] These lawsuits are almost always dismissed for failure to meet the $5,000 loss minimum.[53] Courts justify these dismissals by looking primarily to the CFAA's history as an antihacking statute to determine that the loss of personal information is not a cognizable loss under the statute.[54] Although hundreds of lawsuits claiming the loss of personal privacy have been filed,[55] courts remain reluctant to read the

---

[45] *See, e.g.*, Reuben Fischer-Baum, *What 'Tech World' Did You Grow Up In?*, WASH. POST (Nov. 26, 2017), https://www.washingtonpost.com/graphics/2017/entertainment/tech-generations/ [https://perma.cc/8R5N-P8RD] (select "2008" from dropdown menu following "To customize your experience, enter your birth year" for discussion of technological advances since 2008). For example, in 2008, only 9 percent of Americans owned smartphones, whereas in 2017, 75 percent of Americans owned smartphones. *Id.*

[46] Bhavin Turakhia, *Top 10 Technological Advances of the Past Decade*, FLOCKBLOG (Jan. 7, 2020), https://blog.flock.com/top-technological-advances-of-the-2010s [https://perma.cc/49Q2-VXJC].

[47] PETER G. BERRIS, CONG. RSCH. SERV., R46536, CYBERCRIME AND THE LAW: COMPUTER FRAUD AND ABUSE ACT (CFAA) AND THE 116TH CONGRESS (2020), https://fas.org/sgp/crs/misc/R46536.pdf [https://perma.cc/VJC4-292G].

[48] *See* Nick Akerman, *Why Two District Courts Dismissed Valid Computer Fraud and Abuse Claims for Lack of Jurisdiction*, CASETEXT (Sept. 1, 2010), https://casetext.com/analysis/why-two-district-courts-dismissed-valid-computer-fraud-and-abuse-claims-for-lack-of-jurisdiction-1 [https://perma.cc/32C9-WNJS].

[49] *See id.*

[50] Van Buren v. United States, 141 S. Ct. 1648, 1649 (2021); *see also* 18 U.S.C. § 1030(e)(11).

[51] *See In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1050, 1065, 1068 (N.D. Cal. 2012).

[52] *See, e.g.*, Akerman, *supra* note 48 (discussing lawsuits filed against big companies alleging violations of the CFAA); *see also infra* Part II.

[53] *See* Akerman, *supra* note 48.

[54] *See* Andrews v. Sirius XM Radio, Inc., 932 F.3d 1253, 1263 (9th Cir. 2019).

[55] *See* Jonathan Pollard, *Supreme Court Limits Computer Fraud and Abuse Act (CFAA)*, POLLARD PLLC (June 14, 2021), https://www.pollardllc.com/supreme-court-cfaa-computer-fraud-abuse-act/ [https://perma.cc/GUZ4-837J].

CFAA broadly in a way that would allow these claims to go forward.[56]

This note argues that since personal information is not protected by the CFAA, an amendment to the statute is necessary to close this gap and better protect the fundamental right to privacy. Part I of this note discusses the CFAA and its legislative intent. Part II examines litigation that has been dismissed for not meeting the CFAA's loss requirement and details why this is a problem. Part III provides an overview of the Federal Privacy Act, a federal law that protects American citizens' personal information from misuse by federal government agencies. Finally, Part IV proposes an amendment to the CFAA's loss requirement and definition of "loss." This amendment expands the definition of loss to include the loss of personal privacy while also eliminating the $5,000 threshold. That way, the CFAA will fulfill its purpose as the sole federal statute to combat computer crimes by providing comprehensive protection to individuals in the face of ever-advancing technology.

I. BACKGROUND: HISTORY OF THE CFAA

Long before cookies existed, people would try to gather information about others through hacking. Hacking is an attempt to access or control a computer or other private network without permission.[57] Hacking has been around since the 1800s, albeit in different ways than we imagine today.[58] For example, in the 1800s, people hacked phone companies to misdirect or disconnect calls.[59] The first computer hackers emerged in the 1960s.[60] These hackers aimed at discovering how computer networks operated and sought to improve them.[61]

By the mid-1980s, over ten million computers were in use in the United States.[62] This presented immense opportunity for hackers, resulting in the "golden age" of computer hacking.[63] These hackers no longer wished to discover how computer networks

---

[56] *See id.*; *see also In re iPhone Application Litig.*, 844 F. Supp. 2d at 1068.

[57] *Definition of 'Hacking,'* ECON. TIMES (Nov. 12, 2021, 1:38 AM), https://economictimes.indiatimes.com/definition/hacking [https://perma.cc/L5RX-2PC3].

[58] *The History of Hacking*, THE UF ONLINE PLAZA, http://plaza.ufl.edu/ysmgator/projects/project2/history.html [https://perma.cc/R2PB-8LHW].

[59] *Id.*

[60] *Id.*

[61] Jose Pagliery, *The Evolution of Hacking*, CNN BUS. (June 4, 2015, 9:27 PM), https://www.cnn.com/2015/03/11/tech/computer-hacking-history/index.html [https://perma.cc/S4UY-TJML].

[62] *See The History of Hacking*, *supra* note 58.

[63] *The History of Computer Hacking and How It Has Evolved over the Years*, PRO ONCALL TECH. (Apr. 23, 2015), https://prooncall.com/the-history-of-computer-hacking-and-how-it-has-evolved-over-the-years/ [https://perma.cc/55VP-B6K5].

operated, but instead began using their skills to cause annoyances, such as printing out inordinate amounts of paper at businesses.[64] These hackers were also more sophisticated, and thus, so were the computer crimes they committed.[65] For example, in 1983, a group of six teenagers was able to hack into the Los Alamos National Laboratory, a nuclear weapons research facility in New Mexico.[66] By 1984, it became clear to Congress that hacking was a nationwide problem that needed to be addressed.[67]

This realization prompted Congress to pass the Comprehensive Crime Control Act of 1984 (CCCA).[68] The CCCA is a federal criminal statute meant to address computer-related offenses.[69] The statute "ma[de] it a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer."[70]

Soon after the passing of the CCCA, computers became a popular fixture at universities and businesses.[71] Hackers were no longer targeting only financial institutions and government computers.[72] Some people started hacking to destroy their former employer's company systems in retaliation for being fired.[73] Hackers also began stealing information, such as login credentials or banking and credit card information.[74] It quickly became clear to Congress that stronger and broader legislation was needed to combat new kinds of computer crimes.[75]

In 1986, Congress expanded the CCCA to create the CFAA.[76] The CFAA prohibits knowingly accessing a protected computer without or in excess of authorization.[77] When originally enacted, the

---

[64] *See* Pagliery, *supra* note 61.

[65] *See The History of Computer Hacking and How It Has Evolved over the Years*, *supra* note 63; *see also* Shawn E. Tuma, *What Does the CFAA Mean and Why Should I Care?—a Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 155 (2011) (explaining the first congressional act to control computer hacking covered crimes related to stealing financial records and government information).

[66] *See* Pagliery, *supra* note 61.

[67] *See The History of Computer Hacking and How It Has Evolved over the Years*, *supra* note 63.

[68] Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, tit. II, 98 Stat. 1976; *see* PROSECUTING COMPUTER CRIMES, *supra* note 44, at 1.

[69] *See* PROSECUTING COMPUTER CRIMES, *supra* note 44, at 1.

[70] *Id.*

[71] *Timeline of Computer History*, COMPUT. HIST. MUSEUM, https://www.computerhistory.org/timeline/computers/ [https://perma.cc/68X5-4UKA].

[72] *See* Pagliery, *supra* note 61.

[73] *See The History of Computer Hacking and How It Has Evolved over the Years*, *supra* note 63.

[74] *See* Pagliery, *supra* note 61.

[75] *See* Tuma, *supra* note 65, at 155.

[76] *See CFAA Background*, *supra* note 43.

[77] 18 U.S.C. § 1030(a)(1); *see also* 18 U.S.C. § 1030(e)(6) (defining "exceeds authorized access" as accessing a computer with authorization and using such access to obtain or alter information in the computer that the accessor is not entitled to). This definition of

CFAA prohibited unauthorized access of any government-operated or government-affiliated computer, financial institution computer, and computers used in interstate commerce.[78] The CFAA's depth was also demonstrated in the many new provisions Congress added, such as one that "penalize[d] those who intentionally alter[ed], damage[d], or destroy[ed] data belonging to others."[79] In expanding the CCCA and creating the CFAA, Congress made clear that the statute's purpose was "to address federal computer-related offenses in a single, new statute."[80]

Despite Congress's attempt to broaden the kinds of computer crimes prohibited under the CFAA, after a few years, it became clear that the CFAA was still too narrow.[81] The CFAA as originally enacted reflected society and technology at the time, mainly protecting those institutions that owned computers, such as "universities, government and military institutions."[82] The CFAA was limited to protecting these institutions because not many people had personal computers in their homes, and if they did, these computers were not normally targeted by hackers.[83] As technology became more affordable, however, it became increasingly common for people to have computer networks in their homes, creating more opportunities for computer-related offenses.[84] This created a gap in the CFAA, as personal computers were not protected under the statute.[85] It became apparent that Congress would need to continually amend the CFAA to close any gaps in the statute's protections that emerged as a result of advancing technology and changing society.[86]

Following this realization, Congress amended the statute in 1994, 2001, and 2008.[87] The most important of these amendments was the 1994 amendment.[88] Congress added this amendment in response to the "dramatic rise in the number of computer crimes

---

"exceeds authorization" has been highly disputed by courts. On June 3, 2021, the Supreme Court determined that an individual exceeds authorized access when they access "a computer with authorization but then obtains information located in . . . areas of the computer . . . that [we]re off-limits to [them]." Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

[78] *What Is the Computer Fraud and Abuse Act?*, FLEESON, GOOING, COULSON & KITCH, LLC (Feb. 10, 2017, 1:32 PM), https://www.fleeson.com/news/fleeson-publications/what-is-the-computer-fraud-and-abuse-act [https://perma.cc/925V-2JQ5].

[79] *See* PROSECUTING COMPUTER CRIMES, *supra* note 44, at 2.

[80] *Id.* at 1.

[81] *See What Is the Computer Fraud and Abuse Act?*, *supra* note 78.

[82] *Id.*

[83] *Id.*

[84] *See The History of Computer Hacking and How It Has Evolved over the Years*, *supra* note 63.

[85] *See* 18 U.S.C. § 1030(e).

[86] S. REP. NO. 104-357, at 5 (1996).

[87] *See CFAA Background*, *supra* note 43; *supra* note 44 and accompanying text.

[88] *See* Tuma, *supra* note 75, at 7.

cases and . . . [prosecutors'] inability to pursue all of the[] claims" made for CFAA violations.[89] The 1994 amendment took pressure off prosecutors by adding a new provision, § 1030(g), which allows private civil remedies.[90] This civil provision aimed to increase the deterrent effect of the statute by providing civilians with a remedy for their losses from computer-related offenses.[91]

Section 1030(g) allows any person who suffers damage or loss because of a violation of this section to bring a civil action against the violator to obtain equitable relief, such as compensatory damages or an injunction.[92] A potential plaintiff may only bring a private civil action if the computer-related offense caused:

> (I) loss to 1 or more persons during any 1-year period. . . aggregating at least $5,000 in value;
>
> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
>
> (III) physical injury to any person; [or]
>
> (IV) a threat to public health or safety.[93]

To bring a private civil action, a person must satisfy at least one of these factors.[94]

Loss as mentioned in the first factor is narrowly defined in § 1030(e)(11), and only includes

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment . . . restoring the . . . information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[95]

The statute allows for the "loss" to be aggregated as long as it stems from "a single act."[96] This means that where the same act affected multiple protected computers, the computers' owners can combine losses to meet the $5,000 threshold.[97] When bringing a

---

[89] Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 92 (2013).

[90] 18 U.S.C. § 1030(g).

[91] *See* Jensen, *supra* note 89, at 92.

[92] 18 U.S.C. § 1030(g).

[93] *Id.* § 1030(c)(4)(A)(i)(I)–(IV).

[94] *Id.* § 1030(g).

[95] *Id.* § 1030(e)(11).

[96] *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 523–24 (S.D.N.Y. 2001) (citing S. REP. NO. 99-132 (1986)).

[97] *Id.* "For example, if someone accessed a White House computer and through that computer erased information on . . . FBI computers, the value of these . . . losses could be aggregated for the purposes of meeting [the statutory minimum]." *Id.* at 524 n.32.

civil action under the first factor in § 1030(g), failure to meet the $5,000 threshold will result in dismissal of the complaint for lack of jurisdiction.[98]

A person may only bring a civil action if their "protected computer" is accessed without or in excess of their authorization, and if one of the four requirements of § 1030(g) is met.[99] Before 2001, a "protected computer" only included financial institution computers, government operated or affiliated computers, "and computers used in interstate or foreign commerce."[100] In 2001, Congress passed the USA PATRIOT Act,[101] which amended the CFAA and broadened the definition of "protected computer" to include "computers located *outside* [of] the United States" and those "used in a manner that affects interstate or foreign commerce . . . [*in*] *the United States*."[102]

Most recently, the 2008 amendment to the CFAA further expanded the definition of "protected computer." The phrase now includes any computer "used in *or affecting* interstate or foreign commerce or communication," meaning the computer no longer had to be in the United States to be protected under the CFAA.[103] This amendment added an extraterritorial element to the CFAA, allowing plaintiffs to bring claims against foreign countries or people.[104] Today, courts have interpreted "protected computer" to include nearly any electronic device that connects to the internet.[105]

The CFAA has been called the "worst law in technology."[106] Its critics claim that the law is vague and outdated, and some have even called for its repeal.[107] While Congress has amended the statute to update some of its provisions to combat new computer offenses, constantly

---

[98] *See* Akerman, *supra* note 48.

[99] 18 U.S.C. § 1030(a), (g).

[100] *See What Is the Computer Fraud and Abuse Act?*, *supra* note 78.

[101] Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

[102] *See CFAA Background*, *supra* note 43 (second emphasis added).

[103] *Id.*

[104] William K. Kane & Melissa M. Mikail, *Extraterritorial Application of the Computer Fraud and Abuse Act*, NAT'L L. REV. (July 3, 2020), https://www.natlawreview.com/article/extraterritorial-application-computer-fraud-and-abuse-act [https://perma.cc/W8PJ-YFPW].

[105] *See* GABRIELLE L. GOULD & JUSTIN C. PIERCE, *Practice Note: Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation*, PRAC. L. 1 (2022), Westlaw W-014-6206, (explaining that courts have found electronics such as cell phones, iPads, Kindles, and videogame systems that connect to the internet are protected computers).

[106] Dan Gillmor, *Is the Computer Fraud and Abuse Act the 'Worst Law in Technology'?*, GUARDIAN (Mar. 20, 2013, 11:17 AM) (quoting Wu, *supra* note 1), https://www.theguardian.com/commentisfree/2013/mar/20/computer-fraud-abuse-act-law-technology [https://perma.cc/8E44-6PXW].

[107] *Id.*

advancing technology requires that the statute be amended regularly.[108] The 1994, 2001, and 2008 amendments all reflect Congress's willingness to regularly expand the CFAA to keep it up to date as technology advances. However, because Congress has never amended the statutory definition of "loss," a large gap in the civil provision of the CFAA remains.

II. RECOGNIZING GAPS IN THE CFAA

For years, Americans have tried to utilize the CFAA's civil provision to protect against unwanted intrusions on their laptops and smartphones. As technology has advanced, businesses have found ways to track users' browsing histories and other information to create a more personalized browsing experience.[109] Today, nearly every website, app, and company tracks its users and collects their personal information.[110] Some companies even profit off their users' personal data by selling it to third parties.[111] Oftentimes, companies use cookies to collect information without the user's permission.[112] Other times, users allow a company to collect their personal information, but the company uses that information in a way that was not authorized by the user.[113] These situations have led many civilians to bring class action lawsuits against companies for violating the CFAA.[114]

The CFAA's narrow definition of loss only includes the types specified by the statute, mainly focusing on technological harms, such as the reasonable costs of "responding to an offense" or other "consequential damages incurred because of interruption of service."[115] This limited definition of loss has prevented many Americans from obtaining the relief the CFAA offers, particularly when the claim is based on a loss of personal privacy.[116] First, this

---

[108] *See supra* notes 81–86 and accompanying text.

[109] Shayna Hodkin, *The Internet of Me: Creating a Personalized Web Experience*, WIRED, https://www.wired.com/insights/2014/11/the-internet-of-me/ [https://perma.cc/8BAL-4UGZ].

[110] Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/ [https://perma.cc/2L2Q-DPPZ].

[111] Max Eddy, *How Companies Turn Your Data into Money*, PCMAG (Oct. 10, 2018), https://www.pcmag.com/news/how-companies-turn-your-data-into-money [https://perma.cc/4YZW-986N].

[112] Del Vecchio v. Amazon, No. C11-366-RSL, 2011 WL 6325910, at *1 (W.D. Wash. Dec. 1, 2011).

[113] *See In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1049–50 (N.D. Cal. 2012).

[114] *Id.* at 1051.

[115] 18 U.S.C. § 1030(e)(11).

[116] *See generally* Andrews v. Sirius XM Radio, Inc., 932 F.3d 1253 (9th Cir. 2019) (denying leave to amend a complaint to add a CFAA claim because the plaintiff failed to allege cognizable loss under the statute); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (dismissing valid CFAA claims for failing to allege $5,000 worth of loss).

Part addresses class action lawsuits that courts have dismissed for failure to meet the CFAA's minimum loss requirement, and courts' reasonings for dismissing these claims. Next, this Part discusses why courts choose to read the CFAA narrowly and what courts ignore by doing so. Finally, this Part details what a narrow reading of the CFAA means for future "loss of personal privacy" CFAA claims.

A. Narrow Interpretations of the CFAA Lead to the Dismissal of Valid Civil Claims

In recent years, individuals have filed hundreds of civil lawsuits against companies for violations of the CFAA.[117] Often, plaintiffs claim they suffered a loss of personal privacy because of a company's unauthorized use of their personal data.[118] One way plaintiffs allege the loss of personal privacy is by arguing that they were denied the profits they might have received had they sold their personal information before the big business did.[119] Plaintiffs bring suit under this theory of loss in order to give their personal information a monetary value that meets the $5,000 threshold, allowing their claim to go forward.[120]

For instance, in *Andrews v. Sirius XM Radio, Inc.*, the plaintiff purchased a pre-owned vehicle from a local used car lot.[121] In purchasing the car, the plaintiff entered personal information, such as his name, home address, and phone number, into the car lot's dealer management system (DMS).[122] The car came equipped with Sirius XM Radio, a subscription-based satellite radio service.[123] Shortly after purchasing the car, the plaintiff began receiving unsolicited advertisements asking him to renew the radio subscription.[124] The plaintiff discovered that the car lot and Sirius XM had a separate agreement that provided Sirius XM with customer information stored in the DMS.[125] While the plaintiff provided the car lot with his personal information, he never permitted them to share that information with Sirius XM.[126] The

---

[117] *See* Pollard, *supra* note 55.

[118] *See, e.g.*, Jensen v. Cablevision Sys. Corp., No. 2:17-cv-00100 (ADS)(AKT), 2017 U.S. Dist. LEXIS 158872, at *4, *33–34 (E.D.N.Y. Sept. 27, 2017) (claiming the loss of privacy where defendant broadcast a public Wi-Fi network through the plaintiff's and other class members' personal Wi-Fi routers without authorization in violation of the CFAA).

[119] *See Andrews*, 932 F.3d at 1262.

[120] *Id.* at 1262 n.9.

[121] *Id.* at 1255.

[122] *Id.*

[123] *Id.* at 1256.

[124] *Id.* at 1255.

[125] *Id.* at 1256.

[126] *Id.*

plaintiff filed a class action lawsuit against Sirius XM, alleging a violation of the Driver's Privacy Protection Act of 1994.[127]

After filing the complaint, the plaintiff sought leave to amend to add a civil claim under the CFAA.[128] The plaintiff argued that Sirius XM violated the CFAA because the class was "denied the profits they might have received" by selling the personal information Sirius XM obtained from the dealership, therefore suffering a loss of personal privacy.[129] The district court denied the motion to amend the complaint, reasoning that the "amendment would be futile because the [plaintiff] 'fail[ed] to allege that he ha[d] suffered'" cognizable loss under the statute.[130]

On appeal, the Ninth Circuit rejected the plaintiff's argument, reasoning that the CFAA's narrow definition of loss did not include potential lost profits.[131] The court further explained that the CFAA is historically "an anti-hacking statute, not an expansive misappropriation statute."[132] Therefore, according to the court, the statute could not be expanded to cover a claim like the plaintiff's, where general harms were unrelated to hacking itself.[133] The court declined to expand the CFAA's limited definition of loss to include potential lost profits and affirmed the district court's decision denying leave to amend.[134]

In rejecting the class's theory of loss and holding that only those who suffer a loss directly caused by computer hacking may bring a civil claim under the CFAA, the court read the CFAA's purpose narrowly.[135] This narrow reading does not allow those who suffer general harms, unrelated to hacking, to successfully bring a civil CFAA claim despite apparent invasions of personal privacy.[136]

Plaintiffs have also tried to allege theories of loss different than the one articulated in *Andrews* to prove a company violated the CFAA. In *In re iPhone Application Litigation*, two different classes brought lawsuits against Apple and other application (app) companies for violating the CFAA.[137] Both classes alleged that Apple

---

[127] *Id.*

[128] *Id.*

[129] *Id.* at 1262.

[130] *Id.* at 1256–57 (quoting Andrews v. Sirius XM Radio, Inc., No. ED CV-17-1724 PA (AFMx), 2018 WL 1406911, at *6 (C.D. Cal. Jan. 9, 2018) (second and third alterations in original)).

[131] *Id.* at 1262.

[132] *Id.* at 1263.

[133] *Id.*

[134] *Id.* at 1263–64.

[135] *Id.* at 1263.

[136] *Id.*

[137] *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1048–49 (N.D. Cal. 2012). The app companies named in the lawsuit were Admob, Inc., Flurry, Inc., AdMarval, Inc., Google, Inc., and Medialets, Inc.

and the app companies violated the CFAA by accessing, collecting, and using the classes' personal information from their Apple devices without authorization,[138] but each class had a different argument for why they met the $5,000 loss threshold.

The first class (the iDevice Class) alleged that Apple violated the CFAA by allowing the apps to collect personal data from their Apple devices without permission.[139] This personal data included the class's addresses, current locations, zip codes, time zones, genders, ages, unique identifiers assigned to their Apple device, and other app-specific information, such as what a user did while using the app.[140] The iDevice Class claimed that collecting this personal information allowed the defendants to track the users without their permission on an ongoing basis, causing them to suffer a loss of personal privacy.[141]

The second class (the Geolocation Class) alleged that Apple violated the CFAA by intentionally collecting, storing, and transmitting their location data without their consent.[142] The Geolocation Class further alleged that, even when a user switched off the location services setting on their device, Apple continued to monitor and store the location information.[143] As a result of storing the unauthorized geolocation data, the class claimed that the cost of memory space aggregated over the class met the $5,000 statutory minimum.[144]

The Northern District of California found that both classes failed to meet the $5,000 statutory minimum for loss.[145] The court reasoned that the iDevice Class failed to meet the statutory minimum because the type of loss claimed—the loss of personal privacy due to the collection of personal information—did not fall within one of the kinds of loss specified by the statute and required for all civil actions.[146] The court emphasized that personal information does not have any monetary value[147] and that the collection of this information does not constitute loss to users.[148]

---

138 *Id.*

139 *Id.* at 1049–50.

140 *Id.* at 1050.

141 *Id.*

142 *Id.*

143 *Id.* at 1050–51.

144 *Id.* at 1066.

145 *Id.* at 1067–69.

146 *Id.* at 1068; *see also* Jensen v. Cablevision Sys. Corp., No. 2:17-cv-00100 (ADS)(AKT), 2017 U.S. Dist. LEXIS 158872, at *34 (E.D.N.Y. Sept. 27, 2017) (finding the invasion of privacy and increased security risks are not "cognizable economic losses under the CFAA").

147 *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1068.

148 *Id.* (citing Bose v. Interclick, Inc., No. 10 Civ. 9183 (DAB), 2011 U.S. Dist. LEXIS 93663, at *4 (S.D.N.Y Aug. 17, 2011)); *see also* Del Vecchio v. Amazon.com Inc., No. C11-366-RSL, 2011 WL 6325910, at *6 (W.D. Wash. Dec. 1, 2011).

The court feared that broadening the CFAA to include the loss of personal privacy would turn the statute into a "sweeping Internet-policing mandate."[149] The court followed binding Ninth Circuit precedent dictating that claims unrelated to hacking, such as loss of privacy claims, are "conclusory" claims that, if protected by the CFAA, would impermissibly expand the statute.[150] The iDevice Class's claim was dismissed with prejudice.[151]

The court also found the Geolocation Class did not have a viable claim under the CFAA.[152] The court reasoned that the Geolocation Class failed to meet the statutory minimum because the device did not function any differently or shut down because of the use of memory space.[153] In declining to adopt a broader version of the CFAA that would include the Geolocation Class's theory of loss, the court again emphasized the CFAA's history as an antihacking statute.[154] The court determined that, in limiting the definition of loss to a few enumerated categories, Congress intended to restrict civil actions to traditional hacking scenarios.[155] These traditional hacking scenarios referred to those where hackers delete information or infect or crash computer networks.[156] Since the class's devices did not function any differently due to the collection of their personal information, the class was not the victim of a "traditional computer 'hacker' scenario" and did not suffer the kind of loss specified in the statute.[157] The Geolocation Class's claim was also dismissed with prejudice.[158]

Other courts have followed the reasoning in *Andrews* and *iPhone Application Litigation*. For example, in *Del Vecchio v. Amazon.com Inc.*, a class of plaintiffs alleged Amazon violated the CFAA by depriving the class of the opportunity to sell their own personal information for profit.[159] The Western District of Washington dismissed the complaint and found that, like in *Andrews*, this theory of loss was entirely speculative, and thus the class did not state a viable claim under the CFAA.[160] The Third Circuit came to a similar conclusion in *In re Google, Inc.*, dismissing

---

[149] Brodsky v. Apple, Inc., 445 F. Supp. 3d 110, 129 (N.D. Cal. 2020) (quoting United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012)).

[150] *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1060.

[151] *Id.* at 1069.

[152] *Id.*

[153] *Id.* at 1067.

[154] *Id.*; *see also* Czech v. Wall St. on Demand, 674 F. Supp. 2d 1102, 1120 (D. Minn. 2009) (citing US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009)).

[155] *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1067.

[156] *Id.*

[157] *Id.*

[158] *Id.* at 1069.

[159] *Del Vecchio*, 2011 WL 6325910, at *2.

[160] *Id.*

a class's claim under the CFAA because the class members failed to show how the defendant's use of their personal information deprived them of appropriating the value for themselves, thus falling short of the $5,000 loss threshold.[161]

Some courts have adopted similar narrow interpretations of the CFAA, albeit for different reasons. In *In re DoubleClick Inc. Privacy Litigation*, a class of plaintiffs claimed DoubleClick violated the CFAA by using cookies to collect and store users' personal information without their permission.[162] The Southern District of New York dismissed the class's claim because the court interpreted the CFAA narrowly, as a statute limited to only "major crimes."[163] In dismissing the claim, the court relied on "Congress' overall intent to limit the CFAA to major crimes"[164] to properly "concentrate Federal resources."[165] The court noted that by imposing the $5,000 minimum, federal resources would be directed to "more substantial . . . offenses that affect interstate or foreign commerce."[166] The Department of Justice (DOJ) has reiterated this interpretation, stating that Congress strictly defined loss to ensure a proper balance between state and federal governments' abilities to prosecute computer crimes.[167]

The court's reasoning in *DoubleClick* reflects Congress's hesitation to create an overly broad CFAA that would render conduct that causes no monetary loss a federal offense. For example, in 2000, Senator Patrick Leahy argued before Congress that a version of the CFAA without the $5,000 loss requirement would make it a federal offense when a college student looks at their teacher's laptop in hopes of seeing their final grade, but "accidentally deletes a file."[168] Prosecuting this, he argued, would be a waste of federal resources.[169] Senator Leahy further argued that the $5,000 floor is consistent with earlier Congress decisions.[170] Specifically, he argued the limit is consistent with a 1986 Senate report, which rejected suggestions that the CFAA be made into a sweeping federal statute to address all computer offenses.[171]

---

[161] *In re* Google Inc., 806 F.3d 125, 149 (3d Cir. 2015).

[162] *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 503, 523 (S.D.N.Y. 2001).

[163] *Id.* at 523–24. "Major crimes" include only those computer offenses that would be considered felonies. *See id.* at 522 n.30.

[164] *Id.* at 523–24; *see also id.* at 522 n.30.

[165] 106 Cong. Rec. S8858–59 (daily ed. Sept. 20, 2000) (statement of Sen. Patrick Leahy).

[166] *Id.*

[167] *See* PROSECUTING COMPUTER CRIMES, *supra* note 44, at 1.

[168] *See* 106 Cong. Rec. S8859 (daily ed. Sept. 20, 2000) (statement of Sen. Patrick Leahy).

[169] *Id.*

[170] *Id.*

[171] *Id.*

Each of these cases reveals that courts are reluctant to expand the CFAA to include the loss of personal privacy for a variety of reasons. Some courts believe that the CFAA should remain true to its history as an antihacking statute, only covering losses directly caused by traditional hacking scenarios.[172] Others are concerned that expanding the statute will turn the CFAA into a "sweeping Internet-policing mandate."[173] Finally, courts and Congress alike have expressed concern that expanding the statute will cause the government to prosecute low-level computer crimes, wasting federal resources.[174]

These cases also reveal that Americans have tried to utilize the civil protections the CFAA offers but have been unsuccessful. Claims against companies that have collected personal information without authorization have been dismissed because of the CFAA's loss requirement and its narrow definition of loss.[175] This has left Americans with no federal civil remedy against big businesses that collect and sell their personal information without authorization.[176]

B. Narrow Interpretations of the CFAA Ignore Problems that May Arise Due to Advancing Technology and Changing Society

In construing the CFAA so narrowly, courts have ignored key changes in the statute that show that Congress intended to broaden its scope. Congress amended the CFAA in 1994, 2001, and 2008 to combat new kinds of computer offenses that emerged because of changing technology.[177] These new offenses Congress sought to prevent were not only traditional hacking crimes, but

---

[172] *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1067.

[173] Brodsky v. Apple, Inc., 445 F. Supp. 3d 110, 129 (N.D. Cal. 2020) (quoting United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012)).

[174] *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 522; 106 Cong. Rec. S8859 (daily ed. Sept. 20, 2000) (statement of Sen. Patrick Leahy).

[175] Andrews v. Sirius XM Radio Inc., 932 F.3d 1253, 1262 (9th Cir. 2019).

[176] *See A Private Right of Action Is Key to Ensuring that Consumers Have Their Own Avenue for Redress*, *supra* note 39. While the plaintiffs in these cases could have brought state claims against the companies, there are disadvantages to doing this. First, not all states where these claims were brought have privacy laws. As of February 11, 2022, only California, Colorado, and Virginia have comprehensive privacy laws. *See* Elizabeth Harding et al., *Tech Transactions and Data Privacy 2022 Report: Look in the Status of Passed, Pending and Failed State Comprehensive Privacy BillsTech*, NAT'L L. REV. (Feb. 11, 2022), https://www.natlawreview.com/article/tech-transactions-data-privacy-2022-report-look-status-passed-pending-and-failed [https://perma.cc/X9V5-KJ5C]. Second, not all these state privacy laws allow for private rights of action. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/LJW3-JM9P]. Bringing a federal civil CFAA action against these companies provides more opportunity for citizens across the country to be protected against unauthorized access to their computers, smartphones, and other electronic devices.

[177] *See supra* Part I.

even included *threatening* to commit a computer-related offense.[178] Further, in the past, narrow versions of the CFAA proved ineffective in combatting computer offenses.[179] Congress purposely broadened the language of the CFAA to render the statute more effective at fighting and deterring computer-related offenses.[180]

Like the court in *Andrews*, the court in *iPhone Application Litigation* also ignored Congress's intent to broaden the CFAA to make it the sole federal statute addressing computer offenses. The court declined to read the statute broadly, citing fear of turning the CFAA into a sweeping statute.[181] In 1994, however, Congress did turn the CFAA into a sweeping statute by amending it to allow criminal prosecutions and private civil actions.[182] Congress also added new kinds of computer-related offenses that the CFAA covered, like trafficking passwords and similar data.[183] Further, the Senate report on the 1996 CFAA amendments (1996 Senate Report) acknowledged that the CFAA would have to continuously be amended to close gaps in the statute as a result of advancing technology.[184] This means that Congress intended for the statute to cover all kinds of computer offenses that emerged as technology advanced, giving the statute broad reach.[185]

Other opponents of broadening the CFAA ignore congressional reports revealing that Congress intended the statute to change as technology advances and new ways of committing computer crimes arise. For example, Senator Leahy's claims ignore the 1996 Senate Report almost completely, even though this report was issued only four years before he argued against the elimination of the $5,000 minimum before Congress.[186] Instead, he relied on the 1986 Senate Report to conclude that the CFAA must be interpreted narrowly.[187] The 1996 Senate Report, however, shows a shift in this attitude, as Congress specifically stated that the CFAA would have to be amended to fight new computer offenses as technology advances.[188] This implies that Congress intended for the statute to

---

[178] *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1067; *CFAA Background*, *supra* note 43.

[179] *See, e.g.*, Jensen v. Cablevision Sys. Corp., No. 2:17-cv-00100 (ADS)(AKT), 2017 U.S. Dist. LEXIS 158872, at *34 (E.D.N.Y. Sept. 27, 2017) (interpreting the CFAA narrowly to dismiss plaintiff's loss of privacy claim).

[180] *See* Jensen, *supra* note 89, at 92.

[181] Brodsky v. Apple Inc., 445 F. Supp. 3d 110, 129 (D. Cal. 2020) (quoting United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012)).

[182] 18 U.S.C. § 1030(g).

[183] *See CFAA Background*, *supra* note 43.

[184] S. REP. NO. 104-357, at 5 (1996).

[185] *Id.* at 10.

[186] *See supra* notes 168–171 and accompanying text.

[187] *See* 106 Cong. Rec. S8859 (daily ed. Sept. 20, 2000) (statement of Sen. Patrick Leahy); *see also supra* note 171 and accompanying text.

[188] S. REP. NO. 104-357, at 5.

be expanded to cover most, if not all, computer offenses. The court in *DoubleClick* also ignored this shifting view by limiting the statute to cover only "major crimes."[189] This interpretation ignores the 1994 amendment, which added a civil cause of action for those who suffered loss as a result of new kinds of computer offenses.[190] A narrow construction of the CFAA ignores congressional reports and amendments to the statute and fails to protect individuals' right to privacy in this new technological age.

C. Implications for Future "Loss of Personal Privacy" CFAA Claims

Some courts acknowledge that Congress has continued to expand the CFAA and have adopted a broad reading of the statute and its minimum loss requirement. In *In re AOL, Inc. Version 5.0 Software Litigation*, the Southern District of Florida acknowledged that the loss of "goodwill and reputation" is a cognizable loss under the CFAA.[191] The court found that while the loss of "goodwill and reputation" does not explicitly fall within one of the categories of loss defined in the CFAA, the statute's history permitted a broader reading.[192] The history the court relied on included the 1996 Senate report, where Congress stated it must remain vigilant to ensure the CFAA is up to date to combat new forms of computer offenses that may emerge in private homes.[193] Additionally, the court relied on statements made by then US Attorney General Janet Reno in which she declared it necessary to strengthen the CFAA to protect more individual computer users.[194] The court recognized that only a broad reading of the CFAA could provide these consumers with protection.[195]

Similarly, in *Ervin & Smith Advertising and Public Relations v. Ervin*, the District Court of Nebraska looked to Congress's intent to broaden the CFAA to find that the "loss of business" is a kind of loss covered by the statute.[196] The court reasoned that limiting "loss" to only the kinds covered by the

---

[189] *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 523–24 (S.D.N.Y. 2001).

[190] *See infra* Part I.

[191] *In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001).

[192] *Id.* at 1374.

[193] *Id.*

[194] *Id.* at 1373 (citing Thurmond v. Compaq Comput. Corp., No. 1:99-CV-0711 (TH/WR), 2001 U.S. Dist. LEXIS 9100, at *21 (E.D. Tex. Mar. 15, 2001)).

[195] *Id.* at 1374.

[196] Ervin & Smith Advert. & Pub. Rels., Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998, at *9 (D. Neb. Feb. 3, 2009).

statute "'would flout Congress's intent' in creating the CFAA."[197] The court went even further to state it would be "nonsensical" to conclude that Congress did not intend to provide a remedy under the CFAA for this kind of loss.[198]

In re AOL and *Ervin* reveal that some courts are willing to give the CFAA and the definition of loss a more expansive reading.[199] However, although hundreds of lawsuits have been brought claiming the loss of personal privacy, no court has interpreted the statute broadly to establish this kind of loss as actionable under the CFAA.[200] In fact, *Andrews*, *iPhone Application Litigation*, and *DoubleClick* show that most courts are reluctant to give the CFAA that broader reading.[201] In each of those cases, the plaintiffs' claims that their protected computers were being accessed without or in excess of their authorization were computer-related offenses that should have been protected under the CFAA. However, because of courts' narrow interpretations of "loss" and Congress's failure to amend the statutory definition of "loss," these claims were dismissed.[202]

III. THE PRIVACY ACT OF 1974 PROTECTS PERSONAL INFORMATION FROM MISUSE BY GOVERNMENT AGENCIES

While no federal law currently protects an individual's personal information from unauthorized collection and use by big businesses,[203] there is a federal law protecting personal information that US government agencies collect and use—the Privacy Act of 1974.[204] The Privacy Act of 1974,[205] also known as the Federal Privacy Act (FPA), is the principal law that governs the relationship between the right to privacy and the government's need to gather information about its citizens.[206] Its purpose is to limit the information the government can collect about its citizens and how that collected information can be

---

[197] *Id.* (quoting EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001)).

[198] *Id.*

[199] *In re Am. Online.*, 168 F. Supp. 2d at 1380.

[200] *Id.* at 1374.

[201] *See supra* Part II.

[202] *Id.*

[203] *See A Private Right of Action Is Key to Ensuring that Consumers Have Their Own Avenue for Redress*, *supra* note 39.

[204] U.S. DEP'T OF JUST., OVERVIEW OF THE PRIVACY ACT OF 1974: 2020 EDITION 1 (2020) [hereinafter US DOJ OVERVIEW OF PRIVACY ACT], https://www.justice.gov/Overview_2020/download [https://perma.cc/6G8Y-KD8C].

[205] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

[206] *Id.* at 1–3.

used, thus protecting people from unwanted invasions of privacy.[207]

The FPA protects citizens in three primary ways. First, it forbids federal agencies from disclosing personal information without consent, except in certain situations.[208] Second, it allows people to request their records and change any records that are not accurate.[209] Under the FPA, a "record" is any information about an individual that is "retrievable by personal identifiers, such as name[or] social security number."[210] Finally, the FPA prohibits agencies from maintaining records that are not "relevant and necessary to accomplish a purpose of the agency."[211]

Unlike the CFAA, the FPA has been broadly construed. The FPA's legislative history clearly states that the word "agency" must be given "its broadest statutory meaning."[212] Additionally, the words "disclosure," "record," and "maintain" as written in the statute are interpreted broadly.[213] The FPA's broad reading is further revealed through the DOJ's comments to § 552a, guidelines written by the Office of Management and Budget (OMB), and courts' interpretations of the FPA.

Under the FPA, "disclosure" of records by federal agencies is forbidden.[214] "Disclosure" is not defined in the statute, but the DOJ and courts have determined that disclosure can occur "by any means of communication."[215] This means a person can disclose information through oral, written, electronic, or any other form of communication and be subject to discipline under the FPA.[216] The DOJ's comments to § 522a(b) indicate that a narrow reading of "disclosure" "would make little sense" given the underlying purpose of the FPA.[217] Courts have followed suit, declaring that "disclosure" should be interpreted broadly to remain true to the FPA's spirit.[218]

---

[207] *Id.* at 1.

[208] *The Privacy Act of 1974*, SOC. SEC. ADMIN., https://www.ssa.gov/privacy/privacy_act_1974.html [https://perma.cc/KEE9-KTTD].

[209] *Id.*

[210] *Id.*

[211] 5 U.S.C. § 552a(e)(1).

[212] 120 CONG. REC. 36,967 (1974) (statement of Rep. William Moorhead), *reprinted in* S. COMM. ON GOV'T OPERATIONS & SUBCOMM. ON GOV'T INFO. & INDIVIDUAL RTS. OF THE H. COMM. ON GOV'T OPERATIONS, 94th Cong., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 3418 (PUB. L. 93-579): SOURCE BOOK ON PRIVACY 958 (1976).

[213] *See* US DOJ OVERVIEW OF PRIVACY ACT, *supra* note 204, at 15–63 (defining key terms in the FPA).

[214] *See supra* note 208 and accompanying text.

[215] *See id.* at 64–65.

[216] *See id.*

[217] *Id.* at 64.

[218] *See* Boyd v. United States, 932 F. Supp. 2d 830, 834 (S.D. Ohio 2013); *see also* Pippinger v. Rubin, 129 F.3d 519, 528–29 (10th Cir. 1997); Wilborn v. Dep't of Health & Hum. Servs., 49 F.3d 597, 600 (9th Cir. 1995).

The word "record" has also been given a broad reading. The OMB guidelines indicate that "record" should be interpreted "to include any record that is linked to an individual through identifying information."[219] Pursuant to these guidelines, the Second, Third, and Fourth Circuits, along with several district courts, have adopted a broad interpretation of the word "record."[220] For example, the District of Columbia Circuit Court found that a videotape was a "record" because it contained a means of identifying a person by their voice.[221] This goes beyond the common meaning of "record" to include things that are not written documents.[222]

The OMB and DOJ have also indicated that the definition of "maintain" has a much broader meaning than its common definition.[223] While the common definition of maintain is "to keep in an existing state,"[224] under the FPA, "maintain" includes activities beyond just "keeping" records, such as gathering and collecting records.[225]

These words are interpreted broadly to remain consistent with the FPA's purpose of balancing the right to privacy against the government's need for information about its citizens.[226] A broad reading of the FPA is necessary to protect personal privacy and ensure there are limits to what the government knows about its citizens.[227] This broad reading is what makes the FPA effective in protecting personal information from government misuse.[228]

The CFAA and FPA are both comprehensive laws addressing the right to privacy. Yet, the courts have given the FPA a broad reading while interpreting the CFAA narrowly.[229] Based on Congress's guidance, the OMB, DOJ, and many courts have declared that a broad reading of the FPA is necessary for the statute to fulfill its purpose and protect the right to privacy. The CFAA, on the other hand, is given a narrow reading that

---

[219] *See* US DOJ OVERVIEW OF PRIVACY ACT, *supra* note 204, at 27–28; *see also* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28,953 (July 9, 1975).

[220] *See* US DOJ OVERVIEW OF PRIVACY ACT, *supra* note 204, at 28.

[221] Albright v. United States, 631 F.2d 915, 920 (D.C. Cir. 1980).

[222] *See Record*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/record [https://perma.cc/Y5K3-M6W9].

[223] *See* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. at 28,948; *see also* US DOJ OVERVIEW OF PRIVACY ACT, *supra* note 204, at 26.

[224] *Maintain*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/maintain [https://perma.cc/DR8Y-7FC9].

[225] *See* US DOJ OVERVIEW OF PRIVACY ACT, *supra* note 204, at 27; *see also* Garris v. Fed. Bureau of Investigation, 937 F.3d 1284, 1295 (9th Cir. 2019).

[226] *Summary of the Privacy Act*, U.S. ENV'T PROT. AGENCY (Nov. 15, 2020), https://www.epa.gov/laws-regulations/summary-privacy-act [https://perma.cc/E72Q-69NC].

[227] *See* US DOJ OVERVIEW OF PRIVACY ACT, *supra* note 204, at 1.

[228] *See id.*

[229] See *supra* Section II.A for discussion of the CFAA's narrow interpretation.

does not allow it to fulfill its purpose of preventing unauthorized access to protected computers to deter computer offenses.[230] Given the need for a broader interpretation of the CFAA, the FPA provides guidance for a solution to the lack of protection the CFAA offers to citizens for the invasion of privacy perpetrated by companies.

IV. CONGRESS SHOULD AMEND THE CFAA TO INCLUDE LOSS OF PERSONAL PRIVACY CLAIMS

To resolve this problem and allow loss of personal privacy claims to proceed past the dismissal for failure to state a claim stage, a new amendment to the CFAA is necessary. First, this amendment should eliminate the $5,000 minimum loss requirement. Under this amendment, § 1030(c)(4)(A)(i)(I), which sets forth the required loss floor, would read "loss to 1 or more persons during any 1-year period . . . *of a kind or kinds specified by the statute*."[231] Eliminating this $5,000 minimum would allow courts to consider types of loss that may not have an easily determined monetary value, such as loss of personal information. Second, this amendment would add "loss of personal privacy" to the statutory definition of loss, found in § 1030(e)(11). Under this amendment, the definition of loss would now be:

> any reasonable cost to any victim, including the [*loss of personal privacy*,] cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to

---

[230] See *supra* Section II.B for discussion of how the CFAA's narrow interpretation fails to fulfill its purpose.

[231] The statute currently reads:

> The punishment for an offense under subsection (a) or (b) of this section is—
>
> . . . .
>
> . . . except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—
>
> . . . an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—
>
> . . . loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value.

18 U.S.C. § 1030(c). This amendment would replace "aggregating at least $5,000 in value" with "of a kind or kinds specified by the statute." 18 U.S.C. § 1030(c)(4)(A)(i)(I).

> the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[232]

The definition of "personal privacy" should be based on the FPA and the US Supreme Court's definition of "personal privacy." Under the FPA, personal "records" include information that is "retrievable by personal identifiers, such as name[or] social security number."[233] In *US Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court "held that the personal privacy concept must encompass an individual's control of information about himself."[234] Therefore, "loss of personal privacy" in this amendment to the CFAA would be defined as "the loss of an individual's control of the information that can be used to identify them."

This is a viable solution because amending the CFAA to broaden the statute is consistent with the congressional intent of creating a single federal statute to combat computer offenses.[235] Congress has acknowledged that the CFAA needs to be continuously amended to combat new kinds of computer offenses.[236] However, the statute was last amended in 2008.[237] A nearly fifteen-year-old amendment cannot account for the vast changes technology and society have undergone since then.[238] Technology has changed nearly every aspect of human life.[239] This advancing technology has also changed hacking. Gone are the days when hackers aimed solely to better computer systems—instead, they now seek to collect highly confidential information.[240]

As technology has advanced, it is not only hackers who can collect this confidential information. Now, companies can track users and collect and sell their personal information for profit or to create personalized browsing experiences.[241] By amending the CFAA to make it an offense for someone to collect, store, or use personal information without or in excess of the user's authorization, critics will no longer be able to claim that the CFAA is "outdated" or the "worst law in technology,"[242]—this

---

[232] 18 U.S.C. § 1030(e)(11). The bracketed text indicates the language this note proposes adding to the statute.

[233] *The Privacy Act of 1974*, *supra* note 208.

[234] Nat'l Archives & Recs. Admin. v. Favish, 541 U.S. 157, 157 (2004) (citing Dep't of Just. v. Reps. Comm. for Freedom of Press, 489 U.S. 749 (1989)).

[235] S. REP. NO. 104-357, at 5 (1996).

[236] *Id.*

[237] *See CFAA Background*, *supra* note 43.

[238] *See* Fischer-Baum, *supra* note 45.

[239] *See* Turakhia, *supra* note 46.

[240] *See* Pagliery, *supra* note 61.

[241] *See* Melendez & Pasternack, *supra* note 22; Freedman, *supra* note 23.

[242] *See* Gillmor, *supra* note 106; Wu, *supra* note 1.

amendment creates a cause of action for a new kind of computer offense that emerged as a result of changing society and technology in recent years.

Additionally, because courts have been so reluctant to broaden their interpretation of the CFAA, this amendment is particularly necessary. Some courts were reluctant to read the statute broadly enough to cover loss of personal privacy claims in fear of disrupting the balance of power and acting as a legislature.[243] Broadening the CFAA to cover loss of personal privacy claims renders this concern moot, striking the proper balance of power between Congress and the courts.

In the cases analyzed above, the plaintiffs' claims that their personal information was collected or used without or in excess of their authorization were computer related offenses that should have been covered by the CFAA.[244] However, courts did not want to place a monetary value on the loss of personal information.[245] By eliminating the $5,000 minimum, courts will not have to consider the value of personal information and the claims can go forward. Further, this amendment will no longer require classes to claim that they were going to sell their personal information for profit but were unable to because the company already did, as the class in *Andrews* was forced to argue.[246] Under the new amendment, all that is relevant is that the personal information was collected without authorization, allowing the claim to proceed.

Some may have concerns that eliminating the $5,000 loss requirement will turn the CFAA into an overly broad, internet policing mandate. This is unfounded. First, eliminating this loss requirement will not affect the balance between state and federal governments' abilities to prosecute computer crimes. Prosecutors have great discretion in deciding what crimes to prosecute.[247] This discretion would allow a prosecutor to choose to only prosecute "major crimes."[248] Also, not all states have internet privacy laws,[249] so this law merely provides more opportunity for Americans to sue companies or individuals who improperly collect their personal information. Further, the

---

[243] *See supra* Part II.A.

[244] *See supra* Part II.C.

[245] *See supra* Part II.B.

[246] See *supra* Part II.A for a discussion of *Andrews*.

[247] *What Is Prosecutorial Discretion?*, FINDLAW (Nov. 12, 2019), https://criminal.findlaw.com/criminal-procedure/what-is-prosecutorial-discretion-.html [https://perma.cc/NB9P-D2W4].

[248] *See A Private Right of Action Is Key to Ensuring that Consumers Have Their Own Avenue for Redress*, *supra* note 39.

[249] *Id.*

CFAA allows for a private right of action, whereas not all state laws do.[250]

Second, eliminating the loss requirement would not automatically allow potential plaintiffs to bring civil actions for all kinds of computer offenses. For example, Senator Leahy's hypothetical situation involving the college student viewing their teacher's laptop in hopes of seeing their final grade would not be actionable under this amended version of the CFAA.[251] A final exam grade is not the kind of information that alone can be used to identify a particular person,[252] and therefore would not fall under the new definition of "loss." The definition of loss would still be narrowly defined, and therefore, this amendment would not "criminalize the conduct of millions of ordinary computer users."[253]

CONCLUSION

Rapidly advancing technology, along with Congress's reluctance to amend the CFAA's definition of loss and courts' narrow interpretations of the statute, have led to a major gap in the CFAA's coverage. This gap has allowed big businesses to collect and sell the personal information of millions of Americans without authorization. To close this gap and better protect personal privacy, it is necessary to take guidance from the FPA and the broad interpretation it is given. Specifically, this note proposes an amendment to the CFAA that eliminates the $5,000 minimum loss requirement and changes the definition of loss to include loss of personal privacy. This amendment will effectively broaden the statute to close this widening gap in the CFAA's coverage that has allowed large companies to collect and sell individuals' personal information since at least 2001. It is likely that as technology advances, Congress will need to continuously amend the CFAA to close

---

[250] *See Status of Internet Privacy Legislation by State*, *supra* note 17; *supra* note 176 and accompanying text; *see also* Allen L. Lanstra, *Exploring the New California Consumer Privacy Act's Unusual Class Action Cure Provision*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (Apr. 23, 2019), https://www.skadden.com/insights/publications/2019/04/quarterly-insights/exploring-the-new-california-consumer-privacy-act [https://perma.cc/N2TW-3T6Z].

[251] *See* 106 Cong. Rec. S8858–59 (daily ed. Sept. 20, 2000) (statement of Sen. Patrick Leahy).

[252] *See* Steve Symanovich, *What Is Personally Identifiable Information (PII)?*, LIFELOCK (Sept. 6, 2017), https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html [https://perma.cc/7B7H-UJ4D].

[253] Jensen v. Cablevision Sys. Corp., No. 2:17-cv-00100 (ADS)(AKT), U.S. Dist. LEXIS 158872, at *27 (E.D.N.Y. Sept. 27, 2017) (quoting United States v. Valle, 807 F.3d 508, 527 (2d Cir. 2015)).

new gaps that arise. This note's proposed amendment closes the current problematic gap. So, at least for now, this proposed CFAA amendment could do something about those annoying, targeted ads that you constantly get on your cell phone.

Alicia Nakhjavan†

† J.D. Candidate, Brooklyn Law School, 2022; B.A., Villanova University 2019. Thank you to the *Brooklyn Law Review* executive board and staff for their hard work and dedication throughout this publication process. Special thanks to my friends for their continued support throughout law school. Finally, thank you to my parents, grandparents, and siblings. I would not be where I am today without your love and support.