

Assignment 1 (Research Paper): Topic Choices

Law #1: Illinois Biometric Information Privacy Act (BIPA) - 2008

DESCRIPTION

Illinois passed the Biometric Information Privacy Act on October 3, 2008, becoming the first state in the nation to create comprehensive rules around how companies collect and use biometric data like fingerprints and face scans (Illinois General Assembly, 2008). The law came about because lawmakers were worried about businesses implementing fingerprint payment systems in grocery stores and gas stations across Illinois without really thinking through the privacy implications. The big concern was that unlike a password or even a Social Security number, you can't just change your fingerprint or face if that data gets stolen or misused.

The law is pretty straightforward in what it requires from companies. Before a business can collect any biometric data - whether that's scanning your fingerprint to clock into work, using facial recognition, or capturing your voiceprint for a voice assistant - they need to get your written permission first (740 ILCS 14/15, 2008). They also have to tell you in writing why they're collecting it, how long they'll keep it, and when they'll finally delete it. Companies can't sell your biometric data to third parties, and they have to use reasonable security measures to protect it.

What makes BIPA unique is that it lets regular people sue companies directly if they violate the law, and they can get money damages without having to prove they were actually harmed (740 ILCS 14/20, 2008). The penalty structure is \$1,000 per violation if the company was careless, or \$5,000 per violation if they did it on purpose. This private right of action has turned BIPA into litigation central - companies have paid out over a billion dollars in settlements since the law passed.

Notable Court Cases

Rosenbach v. Six Flags (2019) - Illinois Supreme Court This case fundamentally changed how BIPA works. A kid went to Six Flags Great America theme park and they scanned his thumbprint for a season pass without getting proper consent from his mom. Six Flags argued that because nothing bad actually happened with the fingerprint data, there was no harm and therefore no case. The Illinois Supreme Court unanimously disagreed, ruling that the statutory violation itself is

enough - you don't have to prove identity theft or some other concrete injury to sue (*Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, 2019). This decision opened the floodgates because it meant that every time a company violates BIPA's procedures, they're potentially on the hook for statutory damages.

Cothron v. White Castle (2023) - Illinois Supreme Court This case addressed a critical question: if an employer scans your fingerprint 100 times without consent, is that one violation or 100 violations? White Castle had employees scanning fingerprints multiple times per day to clock in and out of work, and argued that the first scan was the only violation. The company was also fingered in transferring the biometric details to other third party entities contrary to what BIPA stipulates. The Illinois Supreme Court said no - each scan is a separate violation (*Cothron v. White Castle System, Inc.*, 2023 IL 128004, 2023). White Castle did the math and realized they were potentially facing \$17 billion in damages. The Illinois legislature freaked out and quickly amended BIPA in August 2024 to limit damages to one recovery per person for the same type of violation, but the case shows just how expensive these lawsuits can get.

Rogers v. BNSF Railway (2022) - Federal District Court (Northern District of Illinois) This was the first BIPA case to actually go to trial instead of settling. BNSF Railway Company required truck drivers entering their facilities to scan fingerprints for security access, but they never got consent or even told drivers what they were doing with the biometric data. A jury found that BNSF recklessly violated BIPA over 45,000 times and initially awarded \$228 million in damages (*Rogers v. BNSF Railway Co.*, Case No. 19-cv-03083, N.D. Ill., 2022). The judge later vacated that amount based on *Cothron*, and the case eventually settled for \$75 million. It sent shockwaves through the business community because it proved plaintiffs could actually win at trial with massive verdicts.

In *In re Facebook Biometric Information Privacy Litigation* (N.D. Cal.), plaintiffs alleged that Facebook's "Tag Suggestions" feature used facial recognition to create and store face templates for Illinois users without providing the written notices and consent required under Illinois' Biometric Information Privacy Act (BIPA). The case ended in a \$650 million class action settlement, and the federal court granted final approval on February 26, 2021 (*In re Facebook Biometric Information Privacy Litigation*, 2021). Reporting later indicated that more than 1.42 million Illinois residents filed claims, and many class members received checks that were widely described as around \$345 or more depending on claims administration and deductions (NBC

Chicago, 2022). Overall, the lawsuit showed how expensive it can be for major tech platforms to deploy biometric tools at scale without strict compliance with BIPA (In re Facebook Biometric Information Privacy Litigation, 2021).

Official Link

Illinois General Assembly. (2008). Biometric Information Privacy Act. 740 ILCS 14/1 et seq. Link to Law: <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>

WHAT PART OF THE LAW SEEMS OUTDATED AND WHY

The biggest problem with BIPA is that it lists exactly which biometric identifiers are covered: "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" (740 ILCS 14/10, 2008). This made sense in 2008, when biometric systems were most commonly deployed through **dedicated scanners** in relatively controlled settings (e.g., workplaces or point-of-entry systems). But modern AI systems work totally differently. They create mathematical embeddings from your face or voice - essentially converting your biometric features into a string of numbers that can identify you. Courts are now grappling with whether biometric data **derived from images or audio** - including AI-generated templates/embeddings - falls within BIPA's definitions of a 'scan of ... face geometry' or a 'voiceprint.'. The statute explicitly excludes 'photographs,' which creates a gray area because modern systems can extract biometric identifiers or biometric information **from** ordinary photos or video frames.

The law requires informed written notice and a written release before collection (740 ILCS 14/15(b), 2008), which fits situations where a company can realistically present disclosures to the individual, but it is harder to apply to modern, passive collection. Security cameras with facial recognition scan everyone who walks by. Smart doorbells create face templates of delivery drivers and neighbors without anyone signing anything. Social media platforms extract facial geometry from photos uploaded by other people. The law never contemplated how to get "written consent" from someone whose face appears in their friend's vacation photo that gets uploaded to a platform's servers.

Another gap is the law's silence on AI training data. When companies collect biometric data now, they often use it to train machine learning models that can recognize emotions, predict health conditions, or make hiring decisions. BIPA was written when biometric data was just used for

identification - to confirm you are who you say you are. Nobody in 2008 imagined that companies would use your facial geometry to try to figure out if you're depressed or whether you'd be a good employee. The law doesn't regulate these secondary uses at all.

The "photographs" exclusion has become completely unworkable. The law says regular photographs aren't biometric identifiers, but modern AI can extract highly accurate face geometry from any photo (740 ILCS 14/10, 2008). So companies argue that since they're just processing photographs, BIPA doesn't apply. Taken too broadly, that interpretation could significantly undermine BIPA's protective purpose, since many biometric systems begin with photographs or video frames before generating biometric template. Courts have reached differing conclusions depending on how the technology works and how the data is processed, which has created real uncertainty for companies and consumers

Modernization Recommendations

First, Illinois should update the definition of biometric identifiers to be technology-neutral. Instead of listing specific types, the law should cover "any physiological or behavioral characteristic that can be used to identify an individual with high confidence," including AI-generated embeddings, facial recognition templates, gait analysis, and behavioral biometrics. This would future-proof the law as new identification technologies emerge.

Second, create a tiered consent system based on risk. Low-risk authentication uses (like unlocking your own phone) could use simplified electronic consent, while high-risk uses (surveillance, AI training, emotion detection) should require enhanced consent with clear explanations of risks. For passive collection where individual consent is impossible - like security cameras or photos uploaded by third parties - require opt-out mechanisms and strict limits on how the data can be used.

Third, add specific provisions for AI training data. Require explicit consent before using biometric data to train machine learning models, prohibit inferring sensitive characteristics like health conditions or emotional states without medical-grade consent, and mandate data minimization so companies only keep what they actually need. The law should also require companies to disclose when they're using AI to make decisions about people based on biometric data.

Fourth, fix the electronic consent problem. The 2024 BIPA amendments started this process, but the law should explicitly authorize electronic signatures and clickwrap agreements while requiring companies to make consent mechanisms actually clear and easy to understand - not buried in 50-page terms of service that nobody reads.

Law #2: Video Privacy Protection Act (VPPA) - 1988

DESCRIPTION

Congress passed the Video Privacy Protection Act on November 5, 1988, in direct response to one of the weirdest privacy violations in American history (Video Privacy Protection Act, Pub. L. No. 100-618, 102 Stat. 3195, 1988). When President Reagan nominated Judge Robert Bork to the Supreme Court in 1987, the confirmation hearings got intensely political and nasty. A reporter from the Washington City Paper decided to investigate Bork's character by going to his local video rental store and asking for his rental history. The store just handed it over - no warrant, no subpoena, nothing. The paper published an article listing all 146 movies Bork's family had rented (U.S. Congress, Senate Committee on the Judiciary, 1988). The list was boring - just Cary Grant movies and Alfred Hitchcock films - but Congress was horrified that anyone's video viewing habits could be published that easily.

Congress moved fast and passed VPPA within a year. The law makes it illegal for "video tape service providers" to disclose "personally identifiable information" about what videos a "consumer" rents or buys without that person's written consent (18 U.S.C. § 2710, 1988). Companies that violate it can be sued for at least \$2,500 per violation, plus punitive damages and attorney's fees. In 1988, this clearly meant Blockbuster and other video rental stores couldn't tell people what VHS tapes you rented.

Fast forward to 2022 and the VPPA is experiencing an unexpected second life. Plaintiff's lawyers have filed over 115 lawsuits since 2022 claiming that websites violate VPPA when they embed the Meta Pixel or other tracking technologies (U.S. Congress, Library of Congress, 2023). The argument is that when you watch a video on a news website or streaming platform, the website transmits your viewing information to Facebook, Google, or other advertisers without your

consent. Courts are now trying to figure out whether 1988 language about "video cassette tapes" applies to modern streaming and tracking pixels.

Notable Court Cases

Yershov v. Gannett (2016) - First Circuit Court of Appeals A USA Today app user sued because the app sent her device ID and GPS coordinates to Adobe Analytics along with information about which videos she watched. The First Circuit adopted a broad interpretation of "personally identifiable information," ruling that it includes any data "reasonably and foreseeably likely to reveal which videos a person has obtained" (*Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 1st Cir., 2016). Under this standard, even though Adobe Analytics might not immediately know who the person is, the combination of device ID plus video titles counts as PII because it could be linked to identify someone. The court also said free app users count as "subscribers" even though they don't pay money.

In re Nickelodeon Consumer Privacy Litigation (2016) - Third Circuit Court of Appeals Kids' websites sent cookies and browser information to tracking companies along with what videos children watched. The Third Circuit took the opposite approach from the First Circuit, creating what's called the "ordinary person" test. The court ruled that PII only includes information "that would readily permit an ordinary person to identify a specific individual's video-watching behavior" (*In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 3d Cir., 2016). IP addresses and cookie IDs don't meet this standard because a regular person can't look at an IP address and figure out whose it is. This creates a circuit split that's still unresolved, meaning the same conduct might violate VPPA in Boston but not in Philadelphia.

Eichenberger v. ESPN (2017) - Ninth Circuit Court of Appeals. A Roku user sued ESPN because their app sent his Roku serial number to Adobe Analytics along with which sports videos he watched. The Ninth Circuit sided with the Third Circuit's "ordinary person" standard, holding that Roku serial numbers aren't PII (*Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 9th Cir., 2017). The court acknowledged this is kind of weird: "modern technology may indeed alter, or may already have altered, what qualifies under the statute" to identify someone. But they said Congress needs to update the law; courts can't rewrite it.

Solomon v. Flipps Media (2025) - Second Circuit Court of Appeals This recent case involved news websites embedding Meta Pixel, which sent Facebook User IDs and video viewing data to Facebook. The Second Circuit basically shut down VPPA claims based on tracking pixels, ruling that Facebook User IDs are just "strings of numbers unintelligible to the average person" and don't count as PII (*Solomon v. Flipps Media, Inc.*, No. 23-7597, 2d Cir., 2025). This could effectively kill the recent wave of VPPA litigation, at least in New York and Connecticut.

Official Link

U.S. Congress, 100th Congress. (1988). Video Privacy Protection Act, S. 2361.

<https://www.congress.gov/bill/100th-congress/senate-bill/2361>

Codified at 18 U.S.C. § 2710. <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2710&num=0&edition=prelim>

WHAT PART OF THE LAW SEEMS OUTDATED AND WHY

The entire definition of "video tape service provider" screams 1988. The law literally says it covers entities "engaged in the business of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials" (18 U.S.C. § 2710(a)(4), 1988). Courts have been willing to stretch "similar audio visual materials" to include Netflix and Hulu, but it's awkward. What about TikTok or YouTube? They don't sell or rent videos - they just host them for free(probably). What about a news website that has some videos alongside articles? Is CNN a "video tape service provider" because they have video clips on their website? The law gives no clear guidance.

The "personally identifiable information" definition is equally archaic. It covers "information which identifies a person as having requested or obtained specific video materials" (18 U.S.C. § 2710(a)(3), 1988). This made sense when you walked into Blockbuster and showed your membership card. But modern tracking creates weird edge cases. When you watch a Netflix movie, Netflix knows who you are. But when you watch a video on a news site, the site sends data to dozens of advertising and analytics companies. Those companies get your device ID, cookie ID, IP address, and what video you watched. Does that count? Four circuit courts can't agree.

The law also doesn't account for how advertising technology works now. When VPPA passed, if a video store told someone what you rented, you would know about it because they would have to

actually contact that person. Now, data flows automatically and invisibly. Meta Pixel fires when you load a webpage with a video, sending data to Facebook's servers in milliseconds. You have no idea it happened. The law was designed for deliberate, knowing disclosures to specific people, not automated data sharing with advertising networks.

Another gap is the "consumer" definition: "any renter, purchaser, or subscriber" (18 U.S.C. § 2710(a)(1), 1988). What does "subscriber" mean for free services? If you sign up for a free Hulu account with ads, are you a subscriber? What if you don't sign up for anything and just watch YouTube videos anonymously? The law doesn't say, and courts are split (Interesting).

Modernization Recommendations

First, replace the "video cassette tape" language with modern, technology-neutral definitions. The law should cover "video content providers" - any entity that makes video content available to the public, whether through streaming, download, embedded players, or any other method. This would clearly include Netflix, YouTube, TikTok, news websites with video, and whatever comes next.

Second, update the PII definition to account for modern tracking. Instead of the "ordinary person" test, use a standard similar to COPPA: "information that can be used to contact or identify an individual, including persistent identifiers like IP addresses, device IDs, and advertising IDs." Give the FTC authority to update this definition through rulemaking as tracking technology evolves, rather than relying on courts to stretch 1988 language.

Third, extend liability beyond just the entity disclosing information. Right now, only video providers can be sued under VPPA, not the advertising networks and data brokers who receive and use the viewing data (18 U.S.C. § 2710(b)(1), 1988). This creates a loophole where video providers claim "we're not disclosing PII because device IDs aren't PII" while those device IDs get matched to real identities downstream. Make recipients of viewing data liable too.

Fourth, require transparency about data sharing. Video providers should have to disclose in plain language every third party that receives viewing data, what those companies do with it, and how long they keep it. Give users a simple opt-out mechanism for targeting advertising based on viewing history. This would align VPPA with modern state privacy laws like CCPA that provide opt-out rights.

Law #3: Computer Fraud and Abuse Act (CFAA) - 1986

DESCRIPTION

The Computer Fraud and Abuse Act might be the most important tech law you've never heard of, and it's deeply broken. Congress passed the CFAA on October 16, 1986, as Public Law 99-474, substantially rewriting the narrower 1984 computer fraud law (Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213, 1986). The law's origin story is surprisingly cinematic. In 1983, President Reagan watched *WarGames*, the movie where a teenager accidentally hacks into NORAD's computer systems and nearly starts World War III. Reagan reportedly turned to his national security advisers and asked whether something like that could really happen. The answer scared him enough to push Congress toward creating federal computer crime legislation (U.S. Congress, Congressional Research Service, 2022).

Here's the context that matters: in 1986, only about 2,000 computers were connected to the internet. The law was written for mainframes, room-sized machines with physical access controls and clear ownership boundaries. A "protected computer" meant government servers and bank databases, not the smartphone in your pocket or your smart refrigerator. Nobody imagined a world where virtually every device would be internet-connected and potentially fall under the CFAA's sweeping language (18 U.S.C. § 1030, 1986).

The statute prohibits seven categories of conduct, but the core issues revolve around accessing computers "without authorization" or "exceeding authorized access" to obtain information, cause damage, or commit fraud (18 U.S.C. § 1030(a), 1986). Penalties range from one year to life imprisonment depending on the offense. The massive problem? The law never actually defines what "authorization" means, a gap that has spawned decades of litigation and wildly inconsistent court rulings.

Originally, CFAA covered only government computers and financial institutions. But Congress kept expanding it through amendments in 1988, 1989, 1990, 1994, 1996, and 2001's USA PATRIOT Act (U.S. Congress, Congressional Research Service, 2022). Now it covers essentially any computer connected to the internet or used in interstate commerce, which is basically all of

them. What started as protection for sensitive government systems has become a statute that potentially criminalizes everyday internet activity.

Notable Court Cases

Van Buren v. United States (2021) - U.S. Supreme Court. This case finally forced the Supreme Court to interpret what "exceeds authorized access" actually means under CFAA. Nathan Van Buren was a Georgia police officer who ran a license plate search in a law enforcement database in exchange for money. He definitely had authorized access to the database for his job. He definitely violated department policy by running the search for personal gain. The question was whether misusing authorized access constituted "exceeding authorized access" under CFAA. The Supreme Court ruled 6-3 that it did not (*Van Buren v. United States*, 593 U.S. 374, 2021). Justice Amy Coney Barrett's majority opinion adopted a "gates-up-or-down" test: you "exceed authorized access" only when you access areas of a computer system that are off-limits to you entirely, not when you access permitted information for improper purposes. The critical distinction is between access restrictions (where you can go) and use restrictions (what you can do with information you're allowed to see). This matters enormously because the alternative interpretation would, as Barrett wrote, "attach criminal penalties to a breathtaking amount of commonplace computer activity." But *Van Buren* only partially resolved the chaos, it didn't address what "without authorization" means for public websites, and it left open whether contractual limitations can establish authorization boundaries.

United States v. Aaron Swartz (2013) - Federal District Court (District of Massachusetts). No case better illustrates the CFAA's potential for abuse than the prosecution of Aaron Swartz. Swartz was a programmer and internet activist who co-founded Reddit and helped create RSS. In 2010-2011, while a Harvard research fellow with legitimate access to JSTOR's academic database, Swartz used MIT's network to bulk-download approximately 4.8 million academic articles. When JSTOR and MIT detected and blocked his downloads, he circumvented their blocks and continued. Federal prosecutors charged him with 13 felony counts carrying potential penalties of 35 years in prison and \$1 million in fines (*United States v. Swartz*, Case No. 11-cr-10260, D. Mass., 2013). Think about that: downloading academic articles from a database he was authorized to access could have resulted in more prison time than many violent crimes. JSTOR itself settled with Swartz civilly and didn't push for prosecution, they just wanted him to return the data. But federal

prosecutors pressed forward. On January 11, 2013, Aaron Swartz died by suicide at age 26. The case became a flashpoint for CFAA reform. Representative Zoe Lofgren and Senator Ron Wyden introduced "Aaron's Law" to clarify authorization requirements and prevent prosecutors from stacking charges, but despite multiple reintroductions, Congress has failed to enact meaningful CFAA reform.

United States v. Nosal (Nosal II) (2016) - Ninth Circuit Court of Appeals. This case addressed password sharing, and its holding potentially makes millions of Americans federal criminals. David Nosal was a former executive at Korn/Ferry who used a current employee's login credentials to access company databases after his own access was revoked. The Ninth Circuit found this violated CFAA because only the system owner, not individual employees can grant authorization (*United States v. Nosal*, 828 F.3d 865, 9th Cir., 2016). Judge Stephen Reinhardt's dissent warned the ruling "threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens," potentially making "millions of people who engage in this ubiquitous, useful, and generally harmless conduct into unwitting federal criminals." The implications are staggering: under this interpretation, using someone else's Netflix password, even with their explicit permission, potentially constitutes unauthorized computer access if Netflix's Terms of Service don't approve. First-time CFAA violations can carry five-year sentences. Nobody has actually been prosecuted for sharing a streaming password, and the Department of Justice's 2022 policy explicitly discourages such prosecutions, but it remains theoretically possible.

hiQ Labs v. LinkedIn (2022) - Ninth Circuit Court of Appeals. This case tackled web scraping and whether accessing public data can violate CFAA. hiQ was a data analytics company that scraped publicly available information from LinkedIn profiles to predict employee retention. LinkedIn sent a cease-and-desist letter and blocked hiQ's access. hiQ sued, arguing that scraping public data couldn't violate CFAA because no "authorization" was required to access information anyone could see. The Ninth Circuit agreed - twice. Even after the Supreme Court sent the case back for reconsideration under *Van Buren*, the appeals court reaffirmed that scraping publicly available websites likely doesn't violate CFAA (*hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 9th Cir., 2022). The reasoning follows *Van Buren*'s "gates-up-or-down" framework: if there's no authentication barrier (no password, no login), there's no "authorization" to lack. The case ultimately settled for \$500,000 and a permanent injunction after LinkedIn won on breach of

contract grounds. The lesson: scraping public data is probably fine, but don't create fake accounts or ignore explicit cease-and-desist letters.

Official Link

U.S. Congress, 99th Congress. (1986). Computer Fraud and Abuse Act of 1986, H.R. 4718.

<https://www.congress.gov/bill/99th-congress/house-bill/4718>

Codified at 18 U.S.C. § 1030.

[https://uscode.house.gov/view.xhtml?req=\(title:18+section:1030+edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:18+section:1030+edition:prelim))

WHAT PART OF THE LAW SEEMS OUTDATED AND WHY

The CFAA was written for a world that no longer exists, and nearly every major technological development since 1986 has strained its framework. The most fundamental problem is that the statute never defines "authorization" or "exceeds authorized access" with any precision (18 U.S.C. § 1030(e), 1986). This vagueness has led to decades of inconsistent court interpretations and gives prosecutors enormous discretion to criminalize behavior Congress never intended to punish.

Cloud computing and Software-as-a-Service create impossible questions about authorization. When AWS hosts your company's data alongside thousands of other customers on shared infrastructure, who "owns" the computer being accessed? If a software bug accidentally exposes one tenant's data to another, has a federal crime occurred? The CFAA provides no guidance because it was written for physically distinct mainframes, not virtualized cloud environments where boundaries between "*computers*" are software-defined rather than physical.

APIs might be even more problematic. The modern internet runs on programmatic interfaces that allow applications to communicate. When a developer uses an API, they're accessing someone else's computer systems, but with explicit permission via API keys and authentication tokens. What happens when they violate rate limits or terms of service? After *Van Buren*, purely contractual violations probably aren't CFAA crimes, but the answer remains uncertain. Does exceeding an API rate limit constitute "exceeding authorized access"? Nobody knows for sure.

Security researchers face a particularly absurd situation. Finding and reporting software vulnerabilities, bug bounties, penetration testing, academic security research, often requires

accessing systems in ways their owners didn't explicitly anticipate. The CFAA's vague language means the same activity could be celebrated with a cash reward or prosecuted as a federal felony, depending on a company's mood. Andrew Auernheimer (known as "weev") discovered that AT&T was publicly exposing iPad users' email addresses through a simple URL manipulation. He didn't bypass any passwords or encryptions, just changed a number in a web address. He was sentenced to 41 months in prison (later overturned on jurisdiction grounds, not CFAA interpretation). The chilling effect on security research is profound.

Password sharing represents perhaps the most absurd implication. Under the Ninth Circuit's reading in *Nosal II*, using someone else's streaming service password, even with their explicit permission, potentially constitutes unauthorized computer access if the service provider doesn't approve. Netflix's Terms of Service have historically been ambiguous about sharing. The Department of Justice's 2022 policy explicitly discourages prosecutions for password sharing, but it remains theoretically possible under the statute's current language.

AI and automated data gathering have made these tensions even more acute. Modern AI systems like ChatGPT are trained on massive datasets scraped from the public internet. Yet the legal status of AI training data under CFAA remains unsettled. Is scraping public websites to train AI models unauthorized access if the website owner objects? *hiQ* suggests probably not, but only if the data is truly public and unprotected.

The \$5,000 loss threshold for civil claims hasn't been adjusted since 1986 and should be increased to account for inflation, that \$5,000 in 1986 dollars equals approximately \$14,500-\$14,800 today (18 U.S.C. § 1030(g), 1986). More importantly, courts have interpreted "loss" extremely broadly to include investigation costs and employee time, making the threshold trivially easy to meet and enabling disproportionate prosecutions.

Modernization Recommendations

First, Congress should clearly define "authorization" based on technical barriers rather than contractual terms. Aaron's Law proposed requiring circumvention of "technological or physical measures" (passwords, encryption, locked doors) for criminal liability. This would eliminate the nightmare scenario where violating a website's Terms of Service becomes a federal crime while preserving protection against actual hacking. The distinction should focus on whether someone

bypassed technical access controls, not whether they violated use policies after being granted access.

Second, security research needs explicit safe harbor protection. The DOJ's 2022 policy discouraging prosecution of good-faith researchers is helpful but insufficient, it's just prosecutorial guidance that can change with any administration, and it provides no defense against civil suits. Researchers need statutory protection. Congress should create a safe harbor for security research conducted in good faith to identify and report vulnerabilities, similar to protections in the DMCA for encryption research.

Third, the redundant charging provisions that allowed prosecutors to stack 13 felony counts against Aaron Swartz should be eliminated. The CFAA currently allows multiple charges for essentially the same conduct, creating leverage for prosecutors to threaten devastating sentences and pressure defendants into plea deals. A single course of conduct should result in a single charge, not dozens of stacked felonies.

Fourth, penalties should be proportionate to actual harm. The possibility of decades in prison for downloading academic articles or sharing passwords is absurd on its face. Maximum sentences for non-malicious access violations should be measured in months, not years. The \$5,000 loss threshold should be increased to reflect inflation and courts should be prevented from interpreting "loss" so broadly that any incident response costs trigger federal jurisdiction.

References

18 U.S.C. § 1030 (1986). Fraud and Related Activity in Connection with Computers.
[https://uscode.house.gov/view.xhtml?req=\(title:18+section:1030+edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:18+section:1030+edition:prelim))

18 U.S.C. § 2710 (1988). Video Privacy Protection Act.
<https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2710&num=0&edition=prelim>

740 ILCS 14/1 et seq. (2008). Biometric Information Privacy Act.
<https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>
Biometric Information Privacy Act, 740 ILCS 14/1 et seq. (2008).

Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986).
<https://www.congress.gov/bill/99th-congress/house-bill/4718>

Cothron v. White Castle System, Inc., 2023 IL 128004 (Ill. 2023).

Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017).

hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022).

Illinois General Assembly. (2008). Biometric Information Privacy Act. 740 ILCS 14/1 et seq.
<https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>

In re Facebook Biometric Information Privacy Litigation, Case No. 3:15-cv-03747-JD (N.D. Cal. 2021).

In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3d Cir. 2016).

Rogers v. BNSF Railway Co., Case No. 19-cv-03083 (N.D. Ill. 2022).

Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Ill. 2019).

Solomon v. Flippis Media, Inc., No. 23-7597 (2d Cir. 2025).

U.S. Congress, 99th Congress. (1986). Computer Fraud and Abuse Act of 1986, H.R. 4718.
<https://www.congress.gov/bill/99th-congress/house-bill/4718>

U.S. Congress, 100th Congress. (1988). Video Privacy Protection Act, S. 2361.
<https://www.congress.gov/bill/100th-congress/senate-bill/2361>

U.S. Congress, Congressional Research Service. (2022). Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes. <https://www.congress.gov/crs-product/R47557>

Congressional Research Service. (2019). *Privacy law in the United States* (R45631).
<https://www.congress.gov/crs-product/R45631>

U.S. Congress, Senate Report 100-599. (1988). Video Privacy Protection Act: Report to Accompany S. 2361. <https://www.congress.gov/congressional-report/100th-congress/senate-report/599>

United States v. Nosal, 828 F.3d 865 (9th Cir. 2016).

United States v. Swartz, Case No. 11-cr-10260 (D. Mass. 2013).

Van Buren v. United States, 593 U.S. 374 (2021).

Video Privacy Protection Act, Pub. L. No. 100-618, 102 Stat. 3195 (1988).
<https://www.congress.gov/100/statute/STATUTE-102/STATUTE-102-Pg3195.pdf>

Yershov v. Gannett Satellite Information Network, Inc., 820 F.3d 482 (1st Cir. 2016).