White Knight or Cyber Criminal? The Evolution of Cyber Threats, Protection, and Ethics.

A Thesis in Cyber Security

By: Logan Kleva

Submitted in Partial Fulfillment

of the Requirements

for the Degree of

Bachelor in Arts

With Specialized Honors in Cyber Security

Abstract

Advances in digital technology and the widespread accessibility of computing resources have dramatically expanded the cybersecurity threat landscape, increasing both the scale and complexity of cybercrime. In response, legal systems—particularly in the United States—have relied on statutes such as the Computer Fraud and Abuse Act (CFAA), many of which were drafted in an era of far more limited technological capability. The evolution of technology has not only intensified cybersecurity risk but has also forced a reevaluation of how hacking is defined, prosecuted, and ethically assessed.

Through a comparative analysis of early cybercrime cases and modern cybersecurity disputes, this study examines how technological growth has reshaped the boundary between illegal access and ethically motivated security research. By analyzing landmark court cases, federal policy responses, and evolving cybersecurity frameworks, this paper demonstrates that while early legal approaches favored broad criminalization, contemporary enforcement increasingly recognizes the legitimacy of ethical hacking under defined conditions. Technological evolution has driven both heightened cyber threats and the gradual development of more nuanced legal and ethical standards governing cybersecurity practice.

The legal and ethical boundaries of hacking have been reshaped, allowing for more ethical hacking to take place without the worry of legal injunction, leading to strong reforms and less speculation of the law. Specifically, early technological limitations led to broad, punitive legal frameworks such as the Computer Fraud and Abuse Act, while contemporary cybersecurity threats have forced courts, legislators, and institutions to distinguish more carefully between malicious intrusion and ethically motivated security research. By comparing early cybercrime cases with modern legal disputes and policy reforms, this paper demonstrates how technological evolution has simultaneously increased cyber risk and compelled clearer legal recognition of ethical hacking practice

Table on Contents

I. Introduction

You are going about your day, preparing meals, working a nine-to-five, and managing monthly expenses, when you receive an email warning of a suspicious credit card charge. The message urges immediate action, yet something feels off. After checking your banking app and finding no such transaction, you ignore the message and move on. This moment, though routine, reflects a broader reality: cyber threats have become an ordinary part of modern life.

Individuals and organizations alike are constantly targeted by phishing schemes, credential theft, ransomware, and unauthorized access attempts. While these actions are clearly illegal under existing laws, the methods used to carry them out are often indistinguishable from those employed by cybersecurity professionals acting in defensive or investigative roles. This overlap has created persistent tension between what is legally prohibited and what may be ethically justified.

As digital technology has evolved, so too has this tension. Early cybercrime laws were drafted in response to limited technological capabilities and isolated incidents, resulting in broad statutory language that criminalized unauthorized access with little regard for intent. In contrast, modern cybersecurity environments are defined by professionalized security research, vulnerability disclosure programs, and coordinated defense frameworks. These developments challenge earlier legal assumptions and raise questions about whether ethical hacking should always be treated as criminal conduct.

The legal and ethical boundaries of hacking have been reshaped, allowing for more ethical hacking to take place without the worry of legal injunction, leading to strong reforms and less speculation of the law. By comparing early cybercrime cases with modern legal disputes and policy reforms, this

research demonstrates how technological evolution has both increased cybersecurity risk and compelled more nuanced legal recognition of ethically motivated hacking practices.

II. Definition of Legal and Ethical

When discussing cybercrime, hacking, and security research, it is necessary to clarify what is meant by legal and ethical, not simply as abstract concepts, but as standards that are often applied unevenly in technologically complex environments. Establishing these definitions provides a foundation for understanding why certain actions may be punished under the law while remaining ethically defensible to some observers.

The term legal is generally defined as "conforming to or permitted by law or established rules".[1] In the context of cybersecurity, legality is determined by statutes, regulations, and institutional policies that govern access to computer systems and digital information.[2] These rules are typically written with the goal of preventing harm, protecting property, and maintaining order.[3] However, legal definitions are inherently tied to the technological understanding present at the time they are drafted.[4] As a result, laws governing computer access may struggle to anticipate future use cases, leading to broad or ambiguous language that is later applied to unforeseen scenarios.[5]

By contrast, ethical behavior is defined as "conforming to accepted standards of conduct".[6] Unlike legal standards, ethical judgments are not enforced by courts but are shaped by social norms,

---

[1] "Legal." *Merriam-Webster.com*. (2019)
[2] CRS, "Cybercrime and the Law: Primer on the CFAA" (2026)
[3] U.S. DOJ, "Computer Fraud and Abuse Act" (2022)
[4] Abelson et al., "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." (2015)
[5] Congressional Research Service, "Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes." (2026)
[6] "Ethical." *Merriam-Webster.com*. (2019)

professional expectations, and individual moral reasoning. In cybersecurity, ethical evaluations often focus on intent, harm, and proportionality. For example, an action taken to exploit a vulnerability for personal gain is widely regarded as unethical, whereas a similar action taken to expose a security flaw or prevent future harm may be viewed as ethically justified, even if it violates formal rules.[7]

The tension between these two standards becomes particularly pronounced in digital environments. Computer systems do not operate on human intuition; they operate on permissions, credentials, and technical constraints that may not clearly reflect user intent.[8] Actions such as accessing publicly available data, bypassing rate limits, or testing system defenses can fall into legal gray areas where authorization is ambiguous.[9] In these situations, legality is often determined by strict interpretations of access, while ethical assessments focus on motivation and outcome.[10]

This divergence is not merely theoretical. As digital technology expanded and computer networks became more interconnected, early cybercrime laws were tasked with regulating behavior in systems that were poorly understood by both lawmakers and the public.[11] The result was a legal framework that prioritized broad deterrence over contextual nuance.[12] Understanding how these definitions interact, and sometimes conflict, is essential for evaluating early cyber incidents and the legal responses that followed.

With this framework in mind, examining the earliest signs of cyber attacks reveals how technological limitation, legal uncertainty, and ethical ambiguity shaped the foundation of modern cybercrime law.

---

[7] Ableson et al. (2015)
[8] Kolias et al., “DDoS in the IoT: Mirai and Other Botnets.” (2017)
[9] Sandvig v. Barr (2022)
[10] United States Department of Justice (2022)
[11] Abelson et al. (2015)
[12] Congressional Research Service, Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes, R47557 (2026)

III. Early Cyber Incidents and the Formation of U.S. Cybercrime Policy

To understand where the United States legal system derived its modern cybercrime laws, it is necessary to examine some of the earliest documented cyber attacks and security incidents. These early cases provide insight into how lawmakers and institutions initially perceived computer misuse and why early legal frameworks favored broad deterrence over contextual nuance. By examining these foundational incidents, it becomes easier to understand how legal interpretations of unauthorized access developed and why ethical considerations were largely secondary during this period.

One of the earliest and most influential developments in U.S. cybercrime law was the passage of the Computer Fraud and Abuse Act (CFAA) in 1984.[13] The CFAA was enacted in response to growing concern about unauthorized computer access, particularly following the release of the 1983 film WarGames.[14] The film portrayed a scenario in which a teenager inadvertently accessed a U.S. military computer system and nearly initiated a nuclear conflict. Following the film's release, President Ronald Reagan reportedly questioned whether such an event could occur in reality, prompting heightened concern among policymakers (Congressional Research Service, 2026). These concerns contributed to the creation of a statute designed to broadly criminalize unauthorized access to protected computer systems, even though real-world technological capabilities were far more limited at the time.[15]

The CFAA, codified at Title 18, United States Code, Section 1030, outlines a range of prohibited computer-related activities and has served as the primary federal statute for prosecuting cybercrime for decades.[16] While the law has undergone several amendments since its initial passage, its core language reflects the technological uncertainty and fear that characterized the early era of networked computing.[17]

[13] CRS, Cybercrime and the Law, R47557 (2026)
[14] CRS, Cybercrime and the Law, R47557 (2026)
[15] CRS, Cybercrime and the Law, R47557 (2026)
[16] U.S. Department of Justice (2022)
[17] Abelson et al. (2015)

Rather than narrowly targeting demonstrable harm, the statute emphasized access itself as the primary legal threshold, a feature that would later generate controversy as technology evolved.[18]

One of the earliest and most notable cases prosecuted under the CFAA was the Morris Worm incident in 1988.[19] A computer worm created by Robert Tappan Morris was released onto the early internet and rapidly spread across interconnected systems, including computers at institutions such as MIT, Harvard, Stanford, Princeton, NASA, and the Lawrence Livermore National Laboratory.[20] Although the worm was not designed to destroy files or steal information, it replicated aggressively and significantly degraded system performance across affected networks.[21]

The impact of the Morris Worm was substantial, given the technological limitations of the time. Infected systems slowed to near unusability, disrupting academic and research activities across multiple institutions.[22] Due to the relatively primitive nature of early network defenses and monitoring tools, the spread of the worm was difficult to contain, highlighting the fragility of early interconnected systems.[23] As a result, Morris became the first individual convicted under the CFAA, following amendments made to the statute in 1986 that clarified prosecutorial authority.[24]

From a legal standpoint, Morris's actions clearly violated the CFAA, as he accessed and disrupted computer systems without authorization.[25] Ethically, the case is viewed in a different light. Morris' intent with the worm was to initially test the internet size, and was only intending to infect only once. However, a bug that went undiscovered within the code made it so this worm had a widespread effect. While this was his intent, many still view it as unethical, due to him not getting permission to put this worm on the

[18] United States v. Auernheimer (2014)
[19] Federal Bureau of Investigation (2019)
[20] Federal Bureau of Investigation (2019)
[21] Federal Bureau of Investigation (2019)
[22] Federal Bureau of Investigation (2019)
[23] CRS, Cybercrime and the Law, R47557 (2026)
[24] Congressional Research Service (2026)
[25] Federal Bureau of Intelligence (2019)

system in the first place. Regardless of intent, the widespread disruption caused by the worm demonstrated tangible harm to systems and users, reinforcing the perception that unauthorized access constituted both legal and ethical wrongdoing.[26] This misalignment between legal judgment and ethical evaluation, although an accident, helped solidify early support for strict enforcement of cybercrime laws, as well as showing the laws are not permanent and able to change.

It is important to recognize that these early incidents occurred within a technological environment far less complex than today's digital ecosystem. Early computer systems were characterized by immature security architectures and limited defensive safeguards, making them particularly vulnerable to unintended disruption and exploitation.[27] While a comparable worm introduced into a modern network would likely be detected and contained more rapidly, early systems lacked the layered monitoring, intrusion detection, and coordinated response mechanisms necessary for effective mitigation.[28] This technological context influenced how lawmakers and institutions understood cyber risk and shaped the development of laws that prioritized prevention through broad criminalization.[29]

These early cases illustrate how technological limitations, combined with legal uncertainty, led to a framework that treated unauthorized access as inherently dangerous. Understanding this foundation is critical for evaluating how later cases, arising in far more advanced technological environments, would challenge the adequacy and fairness of early cybercrime law.

IV. Evolution of Technology

As digital technology has advanced, the way computers are built, connected, and used has changed dramatically. Early computers were limited in both capability and connectivity, operating largely

[26] CRS, Cybercrime and the Law, R47557 (2026)
[27] Abelson et al. (2015)
[28] Abelson et al. (2015)
[29] CRS, Cybercrime and the Law, R47557 (2026)

as isolated systems with minimal exposure beyond their immediate users. Over time, improvements in hardware capacity, storage, and processing power enabled more complex applications and broader integration across networks. These technical advancements fundamentally altered not only how systems functioned, but also how they could be accessed, exploited, and defended.

Alongside improvements in hardware, the expansion of global connectivity significantly reshaped the cybersecurity landscape. The commercialization of the internet in the 1990s and the subsequent rise of broadband access connected millions, and eventually billions, of devices worldwide.[30] As digital services expanded across personal, commercial, and governmental domains, the number of potential points of exploitation increased in parallel.[31] Scholars and threat analysts consistently identify a direct relationship between increased connectivity and the expansion of the cyber attack surface, as more systems become reachable through networked interfaces.[32] What once required physical access or specialized institutional credentials could increasingly be attempted remotely, often across national boundaries. Below is a graph illustrating the different kinds of exploitations malicious and ethical hackers alike use to infiltrate systems and get the information they need.

[30] Abdullah et al., "Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data." (2025)
[31] Abdullah et al. (2025)
[32] Abdullah et al. (2025)

Figure 1: The Prime Threats shown in the ENISA Threat Landscape, 2022

The introduction of cloud computing further accelerated this transformation. Organizations began migrating data storage, application hosting, and infrastructure management to centralized cloud service providers in pursuit of scalability and cost efficiency.[33] While this shift offered operational benefits, it also introduced new security challenges related to misconfiguration, shared responsibility, and access control.[34] Under cloud security models, responsibility for safeguarding systems is divided between providers and customers, a structure that has frequently led to ambiguity regarding authorization and accountability.[35] As a result, actions such as accessing exposed cloud storage or improperly secured interfaces may involve unclear boundaries between legitimate access, negligence, and unauthorized intrusion.

[33] Reyes & Mendoza. "Exploring the Impact of Shared Responsibility Models on Cloud Security Posture and Vulnerability Management." (2023)
[34] Reyes & Mendoza (2023)
[35] Reyes & Mendoza (2023)

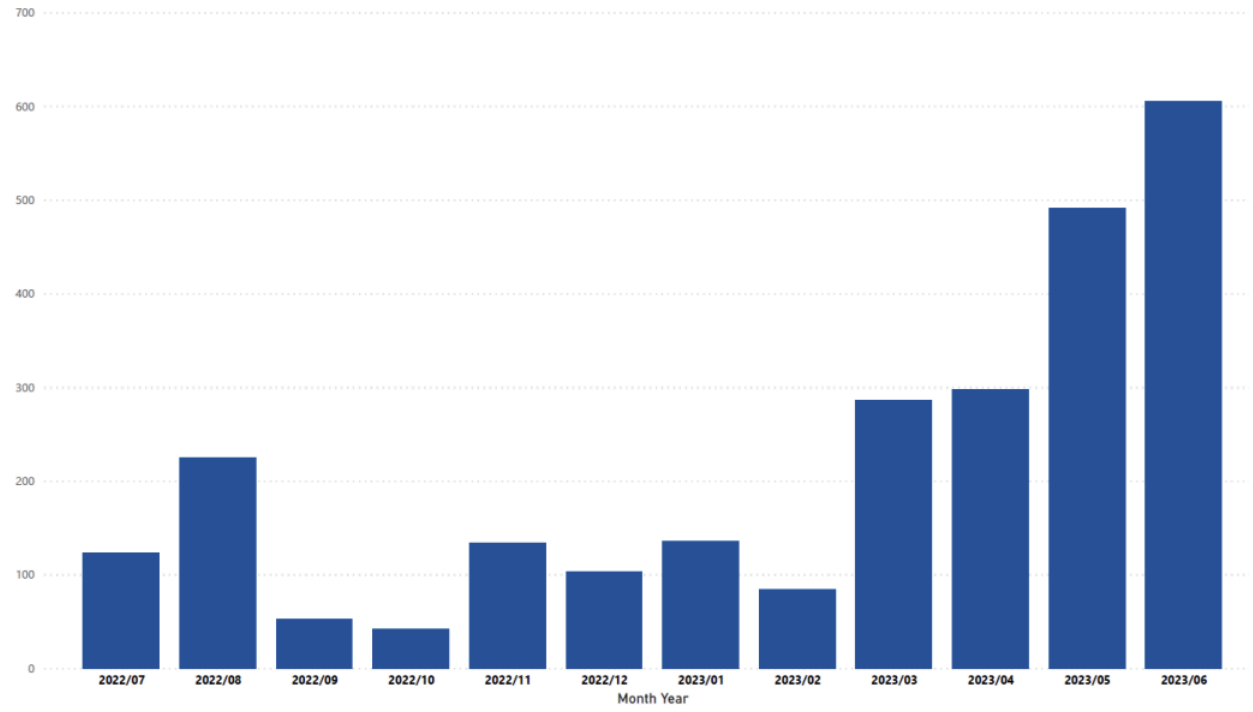

Figure 2: Frequency of Cyber Events per Month in the EU

Although the graph above reflects recorded cyber events within the European Union, it is indicative of broader trends in cyber activity observed across digitally connected regions. As shown in the graph, the period beginning in February 2023 exhibits a marked increase in reported incidents, continuing through June 2023. While the dataset does not extend beyond mid-2023, threat analysts have consistently noted that rising connectivity and expanding digital dependence have corresponded with increased cyber activity across both European and non-European contexts. Accordingly, the graph is best understood as illustrating the pace and concentration of cyber events within a modern networked environment rather than serving as a direct statistical proxy for activity in the United States.

Automation and artificial intelligence have further altered the cybersecurity environment by lowering the technical barrier required to carry out sophisticated attacks. Tools that once demanded advanced programming knowledge can now be deployed at scale through automated scripts and AI-assisted

platforms.[36] At the same time, artificial intelligence has enhanced defensive capabilities through improved detection, monitoring, and pattern recognition.[37] This dual-use nature of AI complicates legal evaluation, as the same technologies can be employed for both protective research and malicious exploitation.[38] As automation accelerates the speed and scale of cyber operations, distinguishing intent becomes increasingly difficult for both technical systems and legal frameworks.

The proliferation of Internet of Things (IoT) devices has expanded cyber risk beyond traditional computing environments and into everyday physical spaces. Smart home systems, wearable devices, industrial sensors, and connected medical equipment often operate with limited security controls due to cost and resource constraints.[39] Research consistently identifies IoT ecosystems as particularly vulnerable to large-scale exploitation, including distributed denial-of-service attacks and botnet formation.[40] The widespread deployment of these devices has created scenarios in which compromised systems may participate in cyberattacks without the owner's knowledge, further complicating questions of responsibility and intent.[41]

Digital financial technologies have also reshaped the structure of cybercrime. The rise of online banking platforms and cryptocurrencies has enabled rapid, cross-border financial transactions while simultaneously complicating law enforcement efforts.[42] Cryptocurrencies, in particular, have been closely associated with ransomware operations due to their pseudonymous nature and ease of transfer.[43] Studies of ransomware ecosystems demonstrate how digital currencies facilitate monetization while reducing the

[36] Maschmeyer, "Deception and Detection: Why Artificial Intelligence Empowers Cyber Defense over Offense." (2026)
[37] Maschmeyer (2026)
[38] Maschmeyer (2026)
[39] Kolias et al. (2017)
[40] Kolias et al. (2017)
[41] Garg et al. "IoT Botnets Unveiled: Architectural Analysis, Threat Vectors, and Cutting-Edge Detection Techniques." (2025)
[42] Tilse & Prasad. "Law Enforcement Challenges in Combating Cybercrime: Digital Forensics and Cryptocurrency on the Dark Web." (2026)
[43] Paquet-Clouston et al., "Ransomware Payments in the Bitcoin Ecosystem." (2019)

risk of attribution and prosecution.[44] These developments highlight how technological innovation can outpace existing legal tools designed to trace and deter criminal activity.

Collectively, these technological changes have placed increasing pressure on legal frameworks originally designed for far simpler systems. Early cybercrime laws treated unauthorized access as a clear indicator of malicious behavior. In modern digital environments, however, access may be automated, indirect, or incidental, and ethical intent may not align neatly with statutory definitions. As systems grow more interconnected and technologically complex, the gap between legal interpretation and ethical evaluation becomes more pronounced. This evolution sets the stage for modern court cases in which existing cybercrime statutes struggle to account for technological context, motivation, and proportional harm.

V. The Risks of Technological Evolution

While technological advancement has enabled unprecedented connectivity and efficiency, it has also introduced new categories of risk that extend beyond traditional notions of cybercrime. As systems grow more powerful and interconnected, vulnerabilities scale alongside them, often faster than legal and regulatory frameworks can adapt. This imbalance between technological innovation and governance has become a defining challenge of modern cybersecurity, placing increasing strain on legal interpretations of responsibility, authorization, and harm.

Ironically, many of the same technological developments that increase cyber risk also enable more sophisticated defensive responses. Advances in system monitoring, logging, and digital forensics have significantly improved the ability of organizations to detect, investigate, and respond to cyber

[44] Paquet-Clouston et al. (2019)

incidents.[45] Modern cybersecurity practices now rely heavily on automated alerts, audit trails, and forensic reconstruction, tools that were largely unavailable during the early development of cybercrime law.[46] These capabilities have enhanced accountability and evidence‑based enforcement, allowing legal institutions to better understand the technical realities underlying cyber incidents.

At the same time, the accelerating pace of technological change continues to generate new risks faster than regulatory systems can accommodate. Emerging technologies such as artificial intelligence, advanced automation, and increasingly complex cloud infrastructures introduce uncertainty regarding attribution, intent, and proportionality. Legal scholars and policy analysts have repeatedly observed that cybersecurity regulation tends to be reactive rather than anticipatory, forming in response to major incidents rather than proactively addressing emerging threats.[47] As innovation cycles shorten, the gap between technological capability and legal oversight widens, increasing the likelihood of enforcement inconsistencies.

Artificial intelligence presents a particularly complex dual‑use dilemma. On one hand, AI has enhanced defensive cybersecurity by improving threat detection, anomaly recognition, and response automation. On the other, the same technologies can be used to generate highly convincing phishing attacks, automate vulnerability discovery, and scale social engineering campaigns.[48] The use of AI complicates legal and ethical assessment because automated actions may obscure human intent, making it difficult to distinguish between malicious exploitation and legitimate security research. As offensive and defensive capabilities increasingly rely on the same tools, traditional legal frameworks struggle to evaluate culpability based solely on access or method.

---

[45] Hodgson et al., Managing Response to Significant Cyber Incidents: Comparing Event Life Cycles and Incident Response Across Cyber and Non‑Cyber Event, RR‑A1265‑4 (2022)
[46] Hodgson et al. (2022)
[47] Congressional Research Service, Federal Cybersecurity: Background and Issues for Congress, R46926 (2024)
[48] Maschmeyer (2026)

The growing interdependence of critical infrastructure further amplifies the risks associated with technological evolution. Energy grids, healthcare systems, transportation networks, and financial institutions are now deeply integrated through digital systems, creating environments in which a single vulnerability can cascade across sectors. Federal risk assessments have warned that cyber incidents targeting critical infrastructure pose threats not only to data security but also to public safety and national stability.[49] In such contexts, the consequences of unauthorized access extend far beyond individual systems, raising questions about how proportionality and harm should be evaluated under existing cybercrime statutes.

Additionally, the widespread adoption of remote work and cloud-based collaboration has reshaped the human dimension of cyber risk. Distributed work environments rely heavily on personal devices, credential-based access, and remote authentication mechanisms, increasing exposure to phishing, credential theft, and social engineering.[50] Annual threat reports consistently identify human error and compromised credentials as dominant initial access vectors, underscoring the persistent role of human vulnerability within technologically advanced systems.[51] These realities challenge legal assumptions that unauthorized access is always the result of deliberate malicious action.

Encryption and anonymity technologies introduce a final layer of ethical and legal tension. Strong encryption safeguards legitimate communications, financial transactions, and personal privacy, forming a cornerstone of modern digital security. However, these same protections can hinder law enforcement investigations by obscuring criminal coordination and complicating attribution. Policymakers continue to debate whether lawful access mechanisms should be required and, if so, how they can be implemented without undermining systemic security. Legal scholarship cautions that efforts to weaken encryption

[49] Cybersecurity and Infrastructure Security Agency, CISA Strategic Plan 2023–2025 (2022)
[50] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023 (Athens: ENISA, 2023).
[51] ENISA, Threat Landscape (2023)

through mandated access mechanisms risk creating vulnerabilities that could be exploited by malicious actors, thereby increasing overall risk.[52]

Ultimately, the risks introduced by technological evolution arise not simply from increased capability, but from increased accessibility. Tools and techniques once limited to governments or highly specialized actors are now widely available through open-source platforms, commercial services, and automated toolkits. This democratization of technical power reshapes both criminal opportunity and ethical responsibility. As a result, legal frameworks originally designed to deter clear-cut malicious behavior are increasingly forced to confront ambiguous cases where intent, harm, and authorization are difficult to disentangle.

As these risks intensified, courts became a primary arena in which the limitations of existing cybercrime statutes were exposed. Judicial decisions increasingly grappled with whether broad legal prohibitions on unauthorized access could be applied fairly within complex technological environments. The following cases illustrate how evolving risk forced the legal system to confront the ethical and practical boundaries of cybercrime law.

VI. Legal–Ethical Conflict in Cybercrime Enforcement

As technological capabilities expanded and cyber risks intensified, the divide between what is legally prohibited and what may be ethically justified became increasingly visible. Nowhere is this tension more apparent than in the enforcement of cybercrime law, where rigid statutory language is often applied to behavior occurring within complex and rapidly evolving technical environments. While early

[52] Ableson et al. (2015)

cyber incidents tended to produce clear alignment between legal judgment and ethical evaluation, modern cases increasingly expose situations in which that alignment breaks down.

In many instances, the legal and ethical ties are split. In the case of Aaron Swartz, whose prosecution under the CFAA further intensified debate surrounding the statute's scope and proportionality. In 2011, Swartz was charged with multiple felony counts for allegedly attempting to download a large volume of academic articles from JSTOR via the MIT network. While JSTOR ultimately declined to pursue charges, federal prosecutors proceeded, citing unauthorized access and circumvention of technical controls. Facing the possibility of decades in prison, Swartz died by suicide in 2013, after which all charges were dropped.[53]

From a strictly legal perspective, Swartz's actions violated institutional policies and technical restrictions, placing him within the CFAA's reach. Ethically, however, the case is widely viewed as emblematic of prosecutorial excess. Swartz's actions caused no permanent damage, financial loss, or data destruction, and JSTOR itself did not view the conduct as warranting criminal punishment. The disconnect between the harm caused and the penalties threatened exposed a structural flaw in the application of cybercrime law, particularly when enforcement fails to account for intent, proportionality, and institutional context.

Another example of the legal and ethical sides being far from each other is United States v. Auernheimer (2014), a case that has become emblematic of CFAA overreach. Andrew "Weev" Auernheimer exploited a vulnerability in AT&T's registration system for early iPad users, which allowed him to collect email addresses associated with customer accounts. Rather than monetizing or misusing the

[53] United States vs. Aaron Swartz (2013)

data, Auernheimer notified AT&T of the flaw and later disclosed the vulnerability publicly after the company failed to respond.[54]

Legally, Auernheimer's actions constituted unauthorized access under the CFAA, as he retrieved information without explicit permission. He was convicted and sentenced to forty-one months in prison, along with significant financial penalties.[55] Ethically, however, the case presents a far more contested narrative. Auernheimer did not bypass authentication mechanisms, steal financial information, or attempt to profit from the data obtained. Instead, his actions resembled what is now commonly recognized as vulnerability research, albeit conducted without formal authorization. The severity of the sentence, combined with AT&T's failure to remediate the vulnerability prior to public disclosure, raised concerns that the law was being used to punish exposure rather than prevent harm.

By contrast, Facebook, Inc. v. Power Ventures, Inc. (2016) illustrates circumstances in which legal and ethical considerations realign. Power Ventures continued accessing Facebook's systems after receiving explicit revocation of authorization and implemented measures to circumvent technical blocks. The Ninth Circuit held that once access permission is clearly revoked, continued circumvention constitutes unauthorized access under the CFAA.[56] In this instance, both legal and ethical frameworks support enforcement, as deliberate evasion of safeguards undermines user trust and platform integrity.

A significant case that addresses ethical research and CFAA liability is Sandvig v. Barr (2020). In this case, academic researchers sought to test whether online platforms engaged in discriminatory practices by creating fictitious accounts in violation of website terms of service. The U.S. District Court for the District of Columbia held that violations of terms of service alone do not constitute criminal access under the CFAA. The court emphasized that allowing private website policies to define criminal liability

[54] United States vs. Andrew Auernheimer (2014)
[55] United States vs. Andrew Auernheimer (2014)
[56] Facebook, Inc. v. Power Ventures, Inc. (2016)

would improperly delegate legislative authority and chill socially valuable research.[57] This decision reflects judicial sensitivity to the ethical necessity of security and civil-rights research, even when such work conflicts with contractual restrictions.

In some instances, legal and ethical assessments remain largely consistent. The SolarWinds supply-chain compromise in 2020 represents a case in which both legal and ethical frameworks clearly converge. SolarWinds, a widely used IT management company, was infiltrated by state-sponsored Russian actors who compromised the company's software update mechanism, distributing malicious code to thousands of downstream customers. According to congressional analysis, approximately 18,000 of SolarWinds' more than 300,000 customers were exposed to the compromised software during the attack window.[58] The intrusion enabled attackers to persist within victim networks, create additional credentials, and access sensitive systems across both the public and private sectors.

In this case, the legal violation is unambiguous. Unauthorized access was achieved through deliberate deception, and the scale of the intrusion produced demonstrable harm to national security, corporate operations, and public trust. Ethical evaluation aligns closely with legal judgment, as the attack lacked any plausible justification beyond espionage and exploitation. Cases such as SolarWinds reinforce the legitimacy of cybercrime statutes when applied to clearly malicious conduct and help establish a baseline against which more ambiguous cases can be evaluated.

More recent judicial decisions suggest growing recognition of these concerns. In Van Buren v. United States (2020), the Supreme Court narrowed the interpretation of the CFAA's "exceeds authorized access" provision, holding that the statute does not criminalize mere misuse of information one is

[57] Sandvig v. Barr (2020)
[58] Congressional Research Service, CRS Insight IN11590 (2021).

otherwise authorized to access. This decision marked a significant shift away from expansive interpretations that had previously allowed routine policy violations to trigger felony liability.[59]

This judicial recalibration is further illustrated in hiQ Labs, Inc. v. LinkedIn Corp. (2019; reaffirmed 2022), a case addressing whether automated scraping of publicly available data constitutes unauthorized access under the CFAA. HiQ, a data analytics firm, collected information from publicly visible LinkedIn profiles to provide workforce analytics services. LinkedIn attempted to block this activity through cease-and-desist letters and technical barriers, asserting CFAA violations. The Ninth Circuit held that accessing publicly available data does not constitute unauthorized access, even after a cease-and-desist letter, emphasizing that expansive CFAA interpretations risk turning the statute into a general-purpose internet policing tool.[60] Ethically, the court's reasoning aligned with modern norms surrounding open data access and research-driven use of publicly shared information.

Collectively, these cases demonstrate that the legal–ethical conflict in cybercrime enforcement is neither hypothetical nor rare. Instead, it reflects a systemic challenge arising from the application of early cybercrime statutes to modern technological contexts. As courts increasingly confront ambiguous cases involving research, data access, and automated systems, judicial interpretation has begun to narrow the scope of the CFAA in ways that better reflect ethical intent and proportional harm. These legal tensions ultimately set the stage for legislative reform and revised prosecutorial guidance, which seek to balance security, innovation, and accountability.

VII. Law Reforms

[59] Van Buren v. United States (2020)
[60] hiQ Labs, Inc. v. LinkedIn Corp. (2022)

As cybercrime law was increasingly applied to technologically complex and ethically ambiguous cases, pressure mounted for reform of the Computer Fraud and Abuse Act. Originally enacted in the 1980s to address a narrow class of computer intrusions, the CFAA's broad language and severe penalties proved ill-suited for modern digital environments. High-profile prosecutions, inconsistent judicial interpretations, and growing concern from the cybersecurity community exposed structural weaknesses in the statute, prompting calls for both legislative and policy-based reform.

One of the most prominent reform efforts emerged in the wake of the Aaron Swartz case. In response to widespread criticism of the CFAA's application, U.S. Senators Ron Wyden and Rand Paul, along with Representative Zoe Lofgren, introduced bipartisan legislation commonly referred to as Aaron's Law. The proposed reform sought to clarify the meaning of "access without authorization" and eliminate the ambiguous phrase "exceeds authorized access," which courts and prosecutors had interpreted expansively.[61] By redefining unauthorized access as the circumvention of technological or physical barriers, rather than violations of contractual terms such as website policies, the bill aimed to prevent the criminalization of routine online behavior and ethically motivated research.

Although Aaron's Law was never enacted, its introduction marked a significant shift in how lawmakers approached cybercrime enforcement. The proposal acknowledged that existing CFAA language granted excessive prosecutorial discretion and enabled disproportionate penalties for conduct that caused little or no harm. Importantly, the reform preserved strong enforcement mechanisms for clearly malicious activity, including malware deployment, denial-of-service attacks, and unauthorized intrusion into protected systems. This distinction reflected growing recognition that cybercrime law must differentiate between malicious exploitation and socially valuable conduct such as security research and academic inquiry.

---

[61] Wyden (2015)

Judicial developments further reinforced the need for reform. Supreme Court and appellate decisions narrowing the scope of the CFAA—most notably Van Buren v. United States and hiQ Labs, Inc. v. LinkedIn Corp.—signaled increasing discomfort with overbroad interpretations of unauthorized access. These rulings emphasized that access restrictions should be understood in terms of technical barriers rather than purpose-based or contractual limitations, aligning legal interpretation more closely with ethical intent and technological reality.

In response to this evolving legal landscape, the Department of Justice implemented significant policy changes governing CFAA prosecutions. In May 2022, the DOJ issued revised charging guidelines directing federal prosecutors to decline prosecution for good-faith security research, even when such research involves technical violations of access restrictions.[62] The policy explicitly discourages cases based solely on violations of terms of service and emphasizes consultation with specialized cybercrime units before charges are brought. While the guidance does not eliminate civil liability or bind future administrations, it represents an institutional acknowledgment that prior enforcement approaches risked chilling legitimate cybersecurity activity.

These reforms reflect an important evolution in how cybercrime law is administered, even in the absence of comprehensive legislative change. Rather than relying exclusively on punitive enforcement, modern approaches increasingly emphasize proportionality, intent, and harm. Courts and prosecutors alike now operate with greater awareness that rigid application of early cybercrime statutes can undermine cybersecurity by discouraging disclosure, research, and innovation. At the same time, reform efforts seek to preserve robust tools for addressing genuinely harmful cyber intrusions.

Ultimately, the trajectory of CFAA reform demonstrates how technological evolution forces legal systems to adapt. While the statute itself remains largely intact, its interpretation and enforcement have

[62] U.S. Department of Justice (2022)

shifted in response to ethical concerns and real-world consequences. These changes underscore the central argument of this paper: that technological advancement not only increases cyber risk, but also compels the development of more nuanced legal and ethical frameworks capable of governing modern digital behavior.

VIII. Impacts on Today's Courts

As courts and policymakers confronted the limitations of early cybercrime statutes, reform increasingly emerged not through wholesale legislative overhaul, but through reinterpretation, judicial narrowing, and revised enforcement policy. Rather than redefining cybercrime law from the ground up, the United States legal system has gradually recalibrated how existing statutes, most notably the CFAA, are applied in cases involving ethically motivated security research. These developments reflect growing recognition that rigid interpretations of unauthorized access risk undermining cybersecurity itself by discouraging vulnerability discovery, disclosure, and defensive testing.

A pivotal moment in this recalibration occurred with the Supreme Court's decision in Van Buren v. United States (2021). The Court rejected expansive interpretations of the CFAA that had permitted criminal liability based solely on misuse of information one was otherwise authorized to access. Instead, the Court held that the statute's "exceeds authorized access" provision applies only when an individual accesses areas of a computer system, such as files, databases, or directories, that are technically off-limits, rather than when access is granted but used for an improper purpose. This narrowing interpretation significantly curtailed the CFAA's reach, preventing routine policy violations or purpose-based misuse from automatically triggering felony liability under federal law. By focusing on technical barriers rather than subjective intent, Van Buren aligned statutory interpretation more closely with both technological reality and ethical assessment.[63]

[63] *Van Buren v. United States*, 593 U.S. 374 (2021)

Judicial clarification alone, however, did not fully resolve the chilling effect faced by security researchers operating in ambiguous authorization environments. In response, the Department of Justice implemented a parallel reform at the enforcement level. In May 2022, the DOJ revised its official charging policy for CFAA cases, explicitly directing federal prosecutors to decline prosecution where the conduct in question constitutes good‑faith security research. The policy defines such research as access undertaken solely for the purpose of testing, investigating, or correcting security vulnerabilities, carried out in a manner designed to avoid harm and intended to promote the safety of systems or their users. Notably, the guidance discourages prosecutions based exclusively on violations of terms of service or contractual access restrictions, emphasizing that criminal enforcement should target malicious circumvention rather than socially beneficial research activity.[64]

Although DOJ charging policies do not carry the force of statutory law and do not foreclose civil litigation or state‑level enforcement, their practical impact is substantial. Federal prosecutors are required to follow these guidelines, and CFAA prosecutions must now undergo heightened review and consultation with specialized cybercrime units. This policy shift represents an institutional acknowledgment that earlier enforcement approaches risked conflating ethical research with criminal intrusion, thereby weakening cybersecurity by discouraging disclosure and defensive innovation. Importantly, the policy preserves robust enforcement authority for clearly malicious conduct, including exploitation for financial gain, extortion, or unauthorized persistence following revocation of access.

Additional legal reinforcement for ethical hacking has emerged through formal authorization mechanisms rather than criminal exemption. Federal agencies increasingly operate vulnerability disclosure programs and bug bounty initiatives that explicitly grant temporary authorization for testing designated systems. Under these frameworks, compliant researchers operate with affirmative permission

[64] U.S. Department of Justice (2022)

rather than relying on prosecutorial discretion. Congressional mandates requiring federal agencies to establish vulnerability disclosure policies further institutionalize this authorization-based approach, recognizing that lawful security research depends on clarity of access rather than after-the-fact adjudication.[65]

Taken together, these reforms reflect an important evolution in U.S. cybercrime governance. Ethical hacking has not been legalized through categorical exemption, nor has the CFAA been fundamentally rewritten. Instead, legality has shifted through narrower judicial interpretation, restrained prosecutorial practice, and explicit authorization structures that transform research activity from unauthorized access into sanctioned defense. This layered approach preserves the statute's deterrent effect against malicious intrusion while reducing the risk that ethically motivated conduct will be met with criminal sanction.

The significance of these reforms extends beyond individual cases. By reducing uncertainty surrounding lawful security research, the legal system encourages earlier vulnerability discovery, coordinated disclosure, and proactive defense—all of which are essential in technologically complex and rapidly evolving digital environments. While tensions between law and ethics in cybersecurity have not been eliminated, contemporary reform demonstrates meaningful movement toward alignment. Ethical intent, proportionality, and technical context now occupy a more central role in determining liability, marking a departure from the broad criminalization that characterized earlier eras of cybercrime enforcement.

[65] 22 U.S.C. § 10306

IX. Conclusion

The evolution of digital technology has fundamentally reshaped the way cybercrime is committed, detected, and regulated. As computing systems expanded from isolated networks into globally interconnected infrastructures, the risks associated with unauthorized access grew in both scale and complexity. In response, legal frameworks such as the Computer Fraud and Abuse Act were applied broadly in an effort to deter harm. However, as this paper has demonstrated, the rapid pace of technological change exposed limitations in early cybercrime law, particularly when rigid legal standards were applied to ethically ambiguous conduct.

By examining the origins of cybercrime legislation, early incidents of unauthorized access, and the subsequent expansion of digital capability, this research shows how technological evolution increased cybersecurity risk while simultaneously challenging traditional legal assumptions. Early cases such as the Morris Worm illustrated a period in which legal and ethical judgments largely aligned. In contrast, modern cases involving vulnerability disclosure, data access, and automated systems reveal growing tension between statutory definitions of unauthorized access and the ethical motivations of security researchers, journalists, and technologists.

The analysis of contemporary court cases further highlights this shift. Decisions in cases such as Auernheimer, Swartz, Van Buren, hiQ Labs, and Sandvig illustrate how courts have struggled to reconcile outdated legal language with modern technological realities. These cases expose a recurring pattern: when cybercrime statutes are applied without consideration of intent, proportionality, or harm, enforcement outcomes risk undermining ethical conduct and discouraging legitimate cybersecurity research. At the same time, cases such as Facebook v. Power Ventures reaffirm that clear revocation of access and deliberate circumvention of safeguards remain firmly within the scope of criminal liability, demonstrating that ethical restraint does not equate to legal immunity.

Reform efforts reflect growing recognition of these challenges. Although legislative proposals such as Aaron's Law have not been enacted, they represent an important acknowledgment that cybercrime law must evolve alongside technology. Similarly, updated prosecutorial guidance from the Department of Justice signals a shift toward more nuanced enforcement, emphasizing good-faith research and discouraging prosecutions based solely on contractual violations. These developments suggest a gradual movement toward legal frameworks that better balance security, accountability, and innovation.

Ultimately, this paper argues that technological evolution does more than increase cyber risk—it forces legal systems to confront the ethical limits of enforcement. As digital tools become more accessible and powerful, the distinction between malicious intrusion and ethically motivated exploration grows increasingly complex. The future of cybersecurity governance will depend on continued refinement of legal standards that recognize this complexity while preserving strong protections against genuine harm. In navigating this balance, law and ethics need not remain in opposition, but must evolve together to ensure a safer and more equitable digital environment.

Sources Cited

Abdullah, Muhammad, et al. “Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data.” *Analytics*, vol. 4, no. 3, 18 Sept. 2025, p. 25, www.mdpi.com/2813-2203/4/3/25?utm, https://doi.org/10.3390/analytics4030025.

Abelson, Harold, et al. “Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications.” *Journal of Cybersecurity*, vol. 1, no. 1, 1 Sept. 2015, pp. 69–79, academic.oup.com/cybersecurity/article/1/1/69/2367066, https://doi.org/10.1093/cybsec/tyv009.

Brundage, Miles . *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. 2018.

CISA. “Indicators Associated with WannaCry Ransomware | CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, 7 June 2018, www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware.

“Cloudflare Research.” *Cloudflare.com*, 2017, research.cloudflare.com/publications/Antonakakis2017/.

Congressional Research Service.

Federal Cybersecurity: Background and Issues for Congress.

CRS Report R46926. Washington, DC: Congressional Research Service, 2024.

Congressional Research Service.

SolarWinds Cyberattack.

CRS Insight IN11590 (2021).

Court, District. “Sandvig v. Barr.” *VLex*, 4 Feb. 2022, case-law.vlex.com/vid/sandvig-v-barr-civil-891252358. Accessed 1 Apr. 2026.

Cornell Law School, Legal Information Institute.
22 U.S.C. § 10306 – Vulnerability Disclosure Policy and Bug Bounty Program Report.
https://www.law.cornell.edu/uscode/text/22/10306

"Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes."
Congress.gov, 2026, www.congress.gov/crs-product/R47557#_Toc135223782.

Cybersecurity and Infrastructure Security Agency.
CISA Strategic Plan 2023–2025.
Washington, DC: Department of Homeland Security, 2022.
https://www.cisa.gov/sites/default/files/2023-06/sp508.pdf.

"Definition of LEGAL." *Merriam-Webster.com*, 2019,
www.merriam-webster.com/dictionary/legal.

"Department of Justice Announces New Policy for Charging Cases under the Computer Fraud
and Abuse Act." *Justice.gov*, 19 May 2022,
www.justice.gov/archives/opa/pr/department-justice-announces-new-policy-charging-cas
es-under-computer-fraud-and-abuse-act.

European Union Agency for Cybersecurity (ENISA).
ENISA Threat Landscape 2023.
Athens: ENISA, 2023.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Facebook Inc. v. Power Ventures Inc. (2016)
https://cdn.ca9.uscourts.gov/datastore/opinions/2016/07/12/13-17102.pdf

Federal Bureau of Investigation. "Morris Worm." *Federal Bureau of Investigation*, 17 July 2019,
www.fbi.gov/history/famous-cases/morris-worm.

"Federal Cybersecurity: Background and Issues for Congress." *Congress.gov*, 2025,
www.congress.gov/crs-product/R46926.

Garg, Umang, et al. “IoT Botnets Unveiled: Architectural Analysis, Threat Vectors, and Cutting-Edge Detection Techniques.” *Cluster Computing*, vol. 28, no. 15, 9 Oct. 2025, https://doi.org/10.1007/s10586-025-05633-1. Accessed 24 Oct. 2025.

Hashizume, Keiko, et al. “An Analysis of Security Issues for Cloud Computing.” *Journal of Internet Services and Applications*, vol. 4, no. 1, 2013, p. 5. *Springeropen*, jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5, https://doi.org/10.1186/1869-0238-4-5.

HiQ Labs, INC v. LinkedIn Corporation (2022) https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf

Hodgson, Quentin E., Aaron Clark‑Ginsberg, Zachary Haldeman, Andrew Lauland, and Ian Mitch.

Managing Response to Significant Cyber Incidents: Comparing Event Life Cycles and Incident Response Across Cyber and Non‑Cyber Events.

RAND Research Report RR‑A1265‑4. Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/pubs/research_reports/RRA1265-4.html.

Kolias, Constantinos, et al. “DDoS in the IoT: Mirai and Other Botnets.” *Computer*, vol. 50, no. 7, 2017, pp. 80–84, ieeexplore.ieee.org/document/7971869, https://doi.org/10.1109/mc.2017.201.

Malatji, Masike, and Alaa Tolah. “Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI.” *AI and Ethics*, vol. 5, 15 Feb. 2024, https://doi.org/10.1007/s43681-024-00427-4.

Maschmeyer, Lennart. “Deception and Detection: Why Artificial Intelligence Empowers Cyber Defense over Offense.” *International Security*, vol. 50, no. 3, 2026, pp. 86–126,

direct.mit.edu/isec/article/50/3/86/135683/Deception-and-Detection-Why-Artificial, https://doi.org/10.1162/isec.a.398.

Monica, 1776 Main Street Santa, and California 90401-3208. “Cybersecurity.” *Www.rand.org*, www.rand.org/topics/cybersecurity.html.

Paquet‑Clouston, Masarah, Bernhard Haslhofer, and Benoît Dupont.

“Ransomware Payments in the Bitcoin Ecosystem.” Journal of Cybersecurity 5, no. 1 (2019): tyz003. https://doi.org/10.1093/cybsec/tyz003.

Reyes, Cristina, and Clarisse Mendoza. “Exploring the Impact of Shared Responsibility Models on Cloud Security Posture and Vulnerability Management.” *Quarterly Journal of Emerging Technologies and Innovations*, vol. 8, no. 1, 2023, pp. 1–10, vectoral.org/index.php/QJETI/article/view/151.

Supreme Court of the United States. *Van Buren v. United States,* 593 U.S. 374 (2021). https://www.supremecourt.gov/opinions/20pdf/19‑783_k53l.pdf

Tilse, Erik, and P. W. C. Prasad. “Law Enforcement Challenges in Combating Cybercrime: Digital Forensics and Cryptocurrency on the Dark Web.” *Lecture Notes in Electrical Engineering*, 2026, pp. 85–94, https://doi.org/10.1007/978-3-032-12170-7_7. Accessed 1 Apr. 2026.

United States vs. Aaron Swartz. https://www.eff.org/files/dmassusvaaronswartzmay13.pdf

“UNITED STATES v. Andrew Auernheimer, Appellant. (2014) | FindLaw.” *FindLaw*, 2026, caselaw.findlaw.com/court/us-3rd-circuit/1663334.html. Accessed 1 Apr. 2026.

U.S. Department of Justice. “Computer Fraud and Abuse Act.” *U.S. Department of Justice*, May 2022, www.justice.gov/jm/jm-9-48000-computer-fraud.

U.S. Department of Justice. “Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act.”, May 19, 2022. https://www.justice.gov/archives/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

“Wyden, Lofgren, Paul Introduce Bipartisan, Bicameral Aaron’s Law to Reform Abused Computer Fraud and Abuse Act | U.S. Senator Ron Wyden of Oregon.” *Senate.gov*, 21 Apr. 2015, www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-?utm. Accessed 1 Apr. 2026.