Voices Unhidden™

Research & Advocacy Publication

The Illusion of Legality

Unauthorized Device Access and the Failure of Enforcement in the Digital Era

---

By Colleen Lawson

Founder, Voices Unhidden™

Publication Date: April 2026
Location: Maryland, United States

About This Publication

This publication examines the growing normalization of unauthorized access to personal digital devices and the systemic challenges that prevent such conduct from being consistently recognized or addressed under existing law.

While federal statutes clearly prohibit unauthorized access to devices and accounts, real-world application reveals a significant gap between legal standards and lived experience. This work explores how that gap is shaped by a combination of interpersonal dynamics, underreporting, inconsistent institutional response, and the increasing influence of commercially available surveillance tools.

Rather than evaluating unauthorized access as isolated incidents, this publication analyzes the broader patterns through which digital monitoring, surveillance, and access-based control operate—particularly within interpersonal relationships. It further examines how these behaviors are normalized, misunderstood, or minimized, despite their alignment with legally defined violations.

By integrating legal analysis, empirical data, and real-world behavioral patterns, this work highlights the need to realign public understanding, institutional response, and commercial accountability with the legal protections that already exist.

Table Of Contents:

SECTION I — INTRODUCTION
SECTION II — LEGAL FRAMEWORK
SECTION III — COMMERCIAL SURVEILLANCE TOOLS AND THE ILLUSION OF LEGALITY
SECTION IV — REAL-WORLD DYNAMICS, UNDERREPORTING, AND INSTITUTIONAL RESPONSE
SECTION V — THE GAP BETWEEN LAW AND ENFORCEMENT
SECTION VI — POLICY, ACCOUNTABILITY, AND AWARENESS IMPLICATIONS
References

Founder’s Introduction

By Colleen Lawson, Founder of Voices Unhidden™

The way individuals experience harm has evolved alongside technology, but the systems designed to recognize and respond to that harm have not kept pace. Increasingly, patterns of monitoring, surveillance, and digital intrusion are being normalized in everyday life—particularly within interpersonal relationships—despite the existence of laws that clearly prohibit unauthorized access to personal devices and accounts.

Through the work of Voices Unhidden™, a recurring theme has emerged: individuals experiencing ongoing digital monitoring or unauthorized access are often uncertain whether what they are experiencing is legally actionable. In many cases, they are met with inconsistent responses when they seek help, leaving them without clear guidance or protection. At the same time, commercially available tools continue to promote the ability to access another person’s digital activity, contributing to widespread confusion about what is permissible.

This publication was developed to address that disconnect. It is not intended to introduce new legal theories, but to clarify what already exists—to examine the legal framework governing unauthorized access, the role of commercial surveillance tools in shaping behavior, and the real-world dynamics that prevent these issues from being consistently recognized or addressed.

As digital technology becomes more deeply embedded in daily life, the ability to distinguish between what is possible and what is lawful becomes increasingly critical. This analysis aims to contribute to that clarity.

SECTION I — INTRODUCTION

The rapid expansion of digital technology has fundamentally reshaped how individuals communicate, form relationships, and access information. Alongside these advancements, however, a quieter and more concerning trend has emerged: the normalization of unauthorized digital surveillance. Across social media platforms, online marketplaces, and commercial advertising spaces, services promoting the ability to monitor another person's phone, read private messages, and track digital activity have become increasingly visible—often presented as accessible, effective, and implicitly lawful.

This normalization exists within a broader landscape of digital harm. Research from the Pew Research Center indicates that **41% of U.S. adults have experienced some form of online harassment**, with **25% reporting exposure to more severe forms**, including stalking, physical threats, and sustained harassment. Notably, **11% of adults report having been stalked online**, highlighting the extent to which digital access can intersect with patterns of targeted harm.

At the same time, data from the Bureau of Justice Statistics demonstrates that approximately **3.4 million individuals age 16 or older were victims of stalking in 2019**, with **67% of victims knowing their offender**, including **25% involving current or former intimate partners**. Despite the scale of this issue, **only 29% of victims reported their victimization to law enforcement**, with reporting rates dropping to **23% in cases involving technology-only stalking**. Among those who did not report, **33% indicated they believed law enforcement could not help**, while **40% stated the incident was not serious enough to report**.

These patterns reveal a critical disconnect between the prevalence of harm and the likelihood of institutional response. As a result, behaviors involving unauthorized access to digital devices and accounts often occur within environments where they are minimized, misunderstood, or treated as interpersonal disputes rather than potential legal violations.

This gap is further reinforced by the increasing availability of commercial surveillance tools. Products marketed as monitoring software, tracking applications, or even "ethical hacking" services promote capabilities that enable access to personal communications, location data, and device activity—often without meaningful consent. The widespread visibility and commercialization of these tools contribute to a broader cultural perception that such conduct is routine, acceptable, or legally permissible.

However, this perception stands in direct conflict with existing federal law. Under statutes such as the Computer Fraud and Abuse Act, accessing a device or account without authorization—or exceeding authorized access—is prohibited, regardless of personal relationships or prior familiarity. Despite the clarity of this legal framework, its application in real-world contexts remains inconsistent, particularly in cases involving known individuals or informal access arrangements.

This paper argues that unauthorized access to personal digital devices is not a legal gray area, but a clearly defined violation that has been obscured by social normalization, commercial influence, underreporting, and inconsistent enforcement. By examining the legal framework, the role of commercial surveillance

tools, and the real-world dynamics that shape reporting and response, this analysis highlights a critical failure to align legal standards with lived reality.

As digital technology becomes increasingly embedded in everyday life, the distinction between what is technically possible and what is legally permissible becomes more important—not less. Without greater clarity, accountability, and institutional consistency, unauthorized digital access will continue to exist in a space where it is widely practiced, commercially supported, and insufficiently addressed.

SECTION II — LEGAL FRAMEWORK

At the federal level, unauthorized access to digital devices is governed primarily by the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030. Originally enacted to address hacking and computer-related offenses, the statute has evolved into a central legal framework for determining when access to digital systems crosses the line from permissible use into unlawful conduct.

The CFAA prohibits both accessing a protected computer "without authorization" and "exceeding authorized access" to obtain information. Courts have interpreted the term "protected computer" broadly to include any device used in or affecting interstate commerce—effectively encompassing modern smartphones, personal computers, and cloud-based accounts. As a result, personal digital devices are afforded the same legal protections as traditional computer systems, regardless of whether they are used in personal or professional contexts.

A central—and frequently misunderstood—component of the statute is the concept of authorization. While the CFAA does not provide a single, comprehensive definition, courts consistently interpret authorization as permission granted by the device owner or system controller. This permission is not unlimited. It may be **explicit or implicit, narrow in scope, conditional in nature, and subject to revocation at any time**.

Importantly, personal relationships do not create automatic or ongoing authorization. The existence of a romantic relationship, shared residence, or prior familiarity with a device does not grant unrestricted legal access to its contents. Authorization must align with the specific scope of permission granted at the time of access. Where access extends beyond that scope—or occurs after permission has been withdrawn—it may fall within the prohibitions of the statute.

This distinction becomes particularly relevant in common, real-world scenarios that are often misinterpreted:

- **Shared Passwords:** Knowing another person's password does not grant unlimited authority to access their accounts. Use beyond the intended or permitted purpose may constitute exceeding authorized access.
- **Prior Access:** Previous permission to use a device does not imply continuing permission. Access after consent has been withdrawn may be unauthorized.
- **Physical Possession:** Having physical access to a device, such as picking up a partner's phone, does not equate to legal authorization to access its contents.
- **Monitoring Software Installation:** Installing tracking or surveillance software on another person's device without their knowledge or consent raises significant legal concerns and may constitute unauthorized access.

The Supreme Court's decision in Van Buren v. United States provides important clarification regarding the interpretation of "exceeding authorized access." The Court held that the CFAA applies when an individual accesses areas of a computer system that are off-limits to them, rather than merely misusing information they were otherwise permitted to obtain. While this decision narrowed certain interpretations

of the statute, it reaffirmed that **access boundaries—not intent alone—are central to determining liability**.

At the same time, courts and enforcement authorities continue to recognize that access obtained without any authorization—particularly through deception, circumvention, or covert means—falls squarely within the statute's prohibitions. This includes scenarios involving the use of another person's credentials without permission, bypassing security measures, or deploying software designed to capture private data without user awareness.

Authorization is also not static. Consent to access a device or account may be withdrawn at any time, and continued access beyond that point may constitute unauthorized access under federal law. This principle is especially significant in interpersonal contexts, where access is often granted informally and later revoked without clear acknowledgment or enforcement.

Despite the clarity of these legal standards, public understanding of authorization remains limited. Many individuals conflate familiarity with permission or assume that relational proximity creates implied access rights. In practice, however, the law draws a clear and enforceable distinction: access must be authorized, and exceeding or bypassing that authorization may carry both civil and criminal consequences.

The persistence of these misconceptions underscores a broader issue: while the legal framework governing unauthorized access is well established, its application to everyday digital interactions remains widely misunderstood. This disconnect contributes directly to the normalization of behaviors that may, in fact, constitute violations of federal law.

SECTION III — COMMERCIAL SURVEILLANCE TOOLS AND THE ILLUSION OF LEGALITY

In parallel with the legal framework governing unauthorized access, a rapidly expanding commercial market has emerged offering tools designed to monitor and track digital activity. These services—commonly marketed as "monitoring software," "tracking applications," or, in some cases, "ethical hacking" tools—provide users with the ability to access another individual's private communications, location data, and device usage, often without the knowledge or meaningful consent of the device owner.

Many of these platforms advertise capabilities that include reading text messages, viewing call logs, tracking GPS location in real time, and remotely accessing content stored on a target device. Federal guidance from the Federal Trade Commission confirms that such tools may enable access to messages, emails, photos, browsing activity, and, in some cases, even allow remote activation of a device's microphone or camera without the user's awareness. These capabilities are not hypothetical—they reflect the actual functionality of products currently available in the marketplace.

While companies frequently position these tools as legitimate for parental oversight or device management, marketing practices often extend well beyond those contexts. Promotional language, user testimonials, and instructional content regularly reference scenarios involving romantic partners or spouses, implicitly suggesting that monitoring another adult's device is reasonable, justified, or even necessary. This framing creates a direct tension with the legal standards outlined in Section II, which require that access be authorized and within the scope of that authorization.

Beyond issues of legality, the proliferation of these tools introduces significant safety risks. By enabling covert, continuous monitoring, they facilitate ongoing surveillance that can be difficult for victims to detect or disrupt. Individuals with minimal technical expertise are able to deploy sophisticated monitoring techniques, effectively lowering the barrier to engaging in invasive conduct. In this way, commercial surveillance tools do not merely reflect existing behaviors—they actively enable and amplify them.

The growing use of such tools is reflected in cybersecurity reporting. Industry data from Kaspersky identified **over 31,000 individuals globally affected by stalkerware in 2023**, representing a measurable increase from the previous year. While these figures likely capture only a portion of actual usage, they demonstrate that the deployment of covert monitoring tools is neither rare nor declining.

A defining feature of this industry is its reliance on legal disclaimers that place responsibility on the end user. Many platforms require users to acknowledge that the product is intended for lawful use and that they must obtain appropriate consent before deployment. However, these disclaimers frequently coexist with marketing strategies that suggest or normalize use cases that may fall outside legal boundaries. This contradiction creates a dual message—one that formally acknowledges legal risk while simultaneously minimizing its perceived significance.

The result is what can be described as an "illusion of legality." The widespread availability, commercialization, and normalization of surveillance tools can lead individuals to assume that their use is

lawful simply because it is accessible and widely promoted. Over time, this perception erodes the distinction between technological capability and legal permissibility.

This dynamic also raises broader questions regarding accountability. While individual users may bear legal responsibility for unauthorized access, the role of companies in designing, marketing, and profiting from tools that enable covert surveillance cannot be overlooked. By presenting invasive monitoring as a productized solution, these companies operate within a space that blurs the line between facilitation and responsibility.

As a result, the rise of commercial surveillance tools represents more than a technological development—it reflects a structural shift in how unauthorized access is enabled, normalized, and perceived. When conduct that may violate federal law is packaged, marketed, and sold as a service, the boundary between what is illegal and what is socially accepted becomes increasingly difficult to distinguish. When unauthorized access is not only possible but productized and commercially promoted, the distinction between legality and availability becomes increasingly obscured.

SECTION IV — REAL-WORLD DYNAMICS, UNDERREPORTING, AND INSTITUTIONAL RESPONSE

Despite the existence of a clearly defined legal framework governing unauthorized access, the real-world application of these protections is significantly shaped by interpersonal dynamics, patterns of underreporting, and inconsistent institutional response. These factors contribute to a persistent gap between what the law prohibits and what is recognized, reported, or addressed in practice.

Data from the Bureau of Justice Statistics indicates that **67% of stalking victims know their offender**, including **25% who identify the offender as a current or former intimate partner**. This demonstrates that a substantial portion of conduct involving unauthorized access and digital monitoring occurs within familiar relationships rather than between strangers. As a result, such behavior is often perceived as a private or interpersonal issue rather than a potential legal violation.

These dynamics directly influence reporting behavior. According to BJS, **only 29% of stalking victims reported their victimization to law enforcement**, with reporting rates declining to **23% in cases involving technology-only stalking**. Among those who did not report, **33% indicated they believed law enforcement could not help**, while **40% stated that the incident was not serious enough to warrant reporting**. These findings reflect not only underreporting, but a broader erosion of confidence in institutional response.

Technology plays a central role in these experiences. Among victims of stalking involving digital tools, BJS found that **22.3% reported being monitored using technologies such as computer or cellphone tracking software**, while **14.4% reported being tracked using an electronic device or application**. These behaviors align directly with the capabilities promoted by commercial surveillance tools, reinforcing the connection between industry practices and real-world harm.

However, the impact of these dynamics extends beyond reporting rates. When individuals do seek assistance, their experiences are often shaped by the way such conduct is interpreted by responding authorities. Reports involving unauthorized access to digital devices—particularly in cases involving known individuals, shared access histories, or the absence of traditional “hacking”—may be minimized, reframed as interpersonal disputes, or deprioritized due to perceived evidentiary challenges. This creates a pattern in which victims encounter not only barriers to reporting, but also a form of institutional dismissal when they attempt to engage with formal systems.

Advocacy organizations, including the National Network to End Domestic Violence, have documented the increasing use of technology as a tool for monitoring, control, and coercion, particularly within abusive or controlling relationships. This pattern is consistent with what is increasingly recognized as technology-facilitated harassment and surveillance, in which access to digital devices becomes a mechanism for ongoing observation, behavioral tracking, and psychological impact over time.

The intersection of these factors—relationship dynamics, underreporting, normalization, and inconsistent response—creates a reinforcing cycle. Unauthorized access occurs, is minimized or misunderstood, goes

unreported or unaddressed, and is therefore perceived as acceptable or inconsequential. This cycle not only obscures the legal nature of the conduct but also allows it to persist without meaningful interruption.

Understanding this cycle is critical. Without acknowledging the real-world conditions under which unauthorized access occurs, legal protections remain underutilized and enforcement mechanisms remain reactive rather than preventative. As digital technology continues to evolve, addressing these dynamics is essential to ensuring that existing legal frameworks are meaningfully applied and that individuals experiencing harm are both recognized and protected.

SECTION V — THE GAP BETWEEN LAW AND ENFORCEMENT

The preceding analysis reveals a fundamental disconnect between legal standards and real-world outcomes. While federal law clearly prohibits unauthorized access to digital devices, the practical enforcement of these protections remains inconsistent, resulting in a widening gap between what the law defines as unlawful and what is recognized or addressed in practice.

At the statutory level, the Computer Fraud and Abuse Act establishes a framework that is both technologically adaptable and sufficiently broad to encompass modern forms of digital access. As outlined in Section II, smartphones, personal devices, and online accounts fall squarely within the scope of protected systems, and unauthorized access—whether through direct intrusion or exceeding granted permissions—is explicitly prohibited.

However, the application of this framework is complicated by the real-world conditions described in Sections III and IV. When **67% of victims know their offender**, and **less than one-third report incidents to law enforcement**, potential violations remain largely outside the scope of formal investigation. This lack of visibility reduces opportunities for enforcement and contributes to the perception that such conduct falls outside the reach of existing law.

At the point of reporting, additional challenges emerge. Law enforcement agencies are often required to assess whether a given incident constitutes a criminal offense, a civil matter, or an interpersonal dispute. In cases involving shared devices, known passwords, or prior access, these distinctions may appear less clear in practice, even when the underlying legal standard—authorization—remains well defined. As a result, unauthorized access may be minimized, deprioritized, or reframed in ways that prevent it from being addressed as a potential violation of federal law.

This enforcement gap is further compounded by the influence of commercial surveillance tools and the normalization of monitoring behaviors. As discussed in Section III, individuals are increasingly exposed to messaging that presents device monitoring as routine or justified. When such messaging is reinforced by the absence of consistent enforcement, it creates a feedback loop in which perceived legality is shaped not by statutory language, but by observed consequences—or lack thereof.

In this environment, the absence of enforcement does not simply reflect a lack of reporting—it contributes to the erosion of legal clarity. When conduct that meets the definition of unauthorized access is repeatedly treated as acceptable or inconsequential, the distinction between legal prohibition and social permission begins to collapse. Individuals may come to rely on availability, accessibility, or common practice as indicators of legality, rather than on the law itself.

This dynamic represents a structural challenge within the current system. Laws such as the CFAA were designed to address unauthorized access from a technical perspective, but they are now being applied within complex interpersonal contexts shaped by evolving norms around privacy, access, and digital boundaries. Without consistent interpretation and application, even well-established legal protections risk becoming functionally ineffective.

Ultimately, the issue is not the absence of legal authority, but the failure to translate that authority into consistent practice. Addressing this gap requires not only reinforcing legal standards, but also improving institutional response, clarifying public understanding, and examining the role of commercial influence in shaping behavior. Until these factors are addressed, unauthorized access will continue to exist in a space where it is clearly prohibited under law, yet inconsistently recognized and insufficiently enforced.

SECTION VI — POLICY, ACCOUNTABILITY, AND AWARENESS IMPLICATIONS

The analysis presented in this paper demonstrates that unauthorized access to digital devices is not a legal ambiguity, but a clearly defined issue within existing federal law. However, the effectiveness of these protections is significantly undermined by gaps in public awareness, inconsistent enforcement, and the normalization of surveillance behaviors through both interpersonal dynamics and commercial influence. Addressing these challenges requires a coordinated response that extends beyond statutory language and into education, enforcement practices, and industry accountability.

A critical first step is improving public understanding of what constitutes unauthorized access. As demonstrated, many individuals continue to operate under the misconception that personal relationships, shared access, or technical capability confer legal permission. Public-facing education—through community initiatives, digital literacy programs, and broader awareness campaigns—must clearly communicate that access to a device or account requires authorization and that such authorization is limited, conditional, and revocable. Increasing awareness serves not only to inform potential victims, but also to prevent violations by correcting widespread misunderstandings.

Equally important is the need for clearer guidance and training within law enforcement and related institutions. Reports involving unauthorized digital access—particularly those occurring within personal relationships—are frequently subject to inconsistent interpretation. Without defined frameworks for assessing issues of authorization, scope, and consent, these cases risk being minimized or misclassified. Providing law enforcement with targeted training on technology-facilitated harassment and surveillance, as well as standardized approaches to evaluating digital access complaints, would improve consistency in response and ensure that potential violations are assessed within the appropriate legal context.

The role of commercial actors must also be addressed. Companies that develop and market monitoring and surveillance tools play a direct role in shaping user behavior and perception. While many platforms rely on legal disclaimers to shift responsibility to the end user, these disclaimers do not negate the impact of marketing strategies that normalize or implicitly encourage unauthorized access. Greater scrutiny of how these tools are advertised, including the use of terms such as “ethical hacking” or “monitoring,” is necessary to ensure that consumers are not misled regarding the legality of their use. Consideration should also be given to regulatory standards that require clearer disclosures, user education, and limitations on features designed to enable covert surveillance.

In addition to regulatory considerations, there is a need to more fully recognize patterns of behavior associated with technology-facilitated harm. Unauthorized access is often not an isolated act, but part of a broader pattern involving repeated monitoring, behavioral tracking, and psychological impact. Integrating this understanding into both policy discussions and enforcement practices allows for a more accurate assessment of risk and harm, particularly in cases involving ongoing surveillance within interpersonal relationships.

Addressing this issue also requires acknowledging the impact of institutional response on victim behavior. As demonstrated, a significant portion of individuals choose not to report incidents due to a belief that law

enforcement cannot assist them or that their experiences will not be taken seriously. Improving response protocols, increasing transparency in how such cases are handled, and reinforcing the legitimacy of these concerns are essential steps in restoring confidence and encouraging reporting.

Finally, a broader cultural shift is necessary to realign social norms with legal standards. The widespread availability of surveillance tools has blurred the distinction between access and entitlement, particularly in personal relationships. Reestablishing clear expectations around digital privacy, consent, and autonomy is critical to ensuring that technological capability does not redefine acceptable behavior.

Ultimately, the challenge is not the absence of legal protections, but the failure to consistently operationalize them within a rapidly evolving digital environment. By strengthening public awareness, improving institutional response, and examining the role of commercial influence, it is possible to close the gap between law and practice. Doing so is essential not only for enforcing existing protections, but for ensuring that individuals are able to maintain autonomy, privacy, and security within their digital lives. As digital access becomes increasingly embedded in daily life, the failure to distinguish between what is possible and what is permissible will continue to place individuals at risk—unless legal standards, institutional response, and public understanding are brought back into alignment.

Closing Statement

Unauthorized access to personal digital devices is not a new phenomenon, but its normalization within modern society represents a significant shift in both perception and risk. As this publication demonstrates, the legal framework governing such conduct is already well established. The challenge lies not in defining the violation, but in recognizing and responding to it consistently.

The convergence of interpersonal dynamics, commercial influence, and inconsistent enforcement has created an environment in which unauthorized access is increasingly misunderstood, minimized, or overlooked. This not only undermines existing legal protections, but places individuals at continued risk of monitoring, surveillance, and control.

Addressing this issue requires more than awareness—it requires alignment. Legal standards, institutional response, and public understanding must operate within the same framework. Without that alignment, the gap between law and practice will continue to expand.

Voices Unhidden™ remains committed to advancing awareness, education, and advocacy in this space, with the goal of ensuring that technology-facilitated harm is recognized, addressed, and prevented.

References

Bureau of Justice Statistics. (2022). *Stalking victimization, 2019*. U.S. Department of Justice. https://bjs.ojp.gov/content/pub/pdf/sv19.pdf

Federal Trade Commission. (2021). *FTC finalizes order banning SpyFone from surveillance business*. https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-finalizes-order-banning-stalkerware-provider-spyware-business

Federal Trade Commission. (n.d.). *Stalkerware: What to know*. https://consumer.ftc.gov/articles/stalkerware-what-know

Kaspersky. (2024). *The state of stalkerware 2023*. https://www.kaspersky.com/about/press-releases/global-kaspersky-report-reveals-digital-violence-has-increased

National Network to End Domestic Violence. (n.d.). *Technology safety*. https://nnedv.org/content/technology-safety/

Pew Research Center. (2021). *The state of online harassment*. https://www.pewresearch.org/internet/2021/01/13/personal-experiences-with-online-harassment/

Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

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

Breaking the Silence on Digital Violence