



Digital Boundaries in Cybercrime Law: Authorisation, Venue and Extraterritorial Jurisdiction under the Computer Fraud and Abuse Act

Anonymised manuscript for double-anonymised review

Dr. Nader Khalifa^{1*}, Mr. Saifuddin Julfikar Rakib², Mr. Goutham Sai³, Ms. Kruthika Priya Sanga⁴, Ms. Yamini Tirumalasett⁵

^{1*}Academic Teaching Scholar, College of Engineering and Science, Victoria University, Australia.

Abstract

Cybercrime exposes a recurring mismatch between networked conduct and legal rules built around bounded permissions and territorial places. This article develops a two-axis “digital boundaries” framework through a doctrinal comparison of four United States cases: *Van Buren v United States*, *United States v Nosal*, *United States v Auernheimer*, and *United States v Ivanov*. The first axis concerns the boundary of computer authorisation: whether criminal liability turns on an improper purpose, on access to information technically or legally unavailable to the user, or on access after permission has been affirmatively revoked. The second axis concerns territorial allocation: where a cyber offence may be prosecuted when actors, servers, data, victims and harmful effects are distributed across multiple places. The cases show that broad substantive reach cannot substitute for a constitutionally and procedurally valid venue, while a narrow approach to “exceeds authorised access” does not eliminate liability where access has actually been revoked. The article argues that cybercrime law should separate four questions that are often collapsed: system permission, information entitlement, purpose of use, and territorial nexus. It proposes a structured decision model for courts and investigators and identifies complementary organisational controls and cross-border cooperation mechanisms. The resulting framework aims to improve legal certainty without treating every misuse of data as hacking or every downstream effect as sufficient to locate a prosecution. Case-level figures drawn from the decisions and descriptive data from FBI Internet Crime Complaint Center reports are used to illustrate the framework and the scale of the problem; the argument itself remains doctrinal.

Keywords: Cybercrime; CFAA; authorisation; jurisdiction; venue; extraterritoriality; computer misuse

ARTICLE INFO: Received: 18.07.2026 Accepted: 20.07.2026 Published: 07.10.2026

© The Author(s) 2026. Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other thirdparty material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0>

1. Introduction

Computer crime law repeatedly encounters a problem of boundaries. Computer systems are designed around credentials, privileges, interfaces and technical controls, while criminal law asks whether access was authorised, exceeded authorisation, or occurred without authorisation. At the same time, the Internet allows conduct to be initiated in one place, executed through infrastructure in another, and experienced as harm in several more places. The legal system must therefore decide both who crossed a digital boundary and where that crossing is legally cognisable.

The practical stakes of these boundary questions are considerable. Complaints to the FBI's Internet Crime Complaint Center (IC3) exceeded one million for the first time in 2025 (1,008,597), and reported losses rose from US\$4.2 billion in 2020 to US\$20.9 billion in 2025. That is roughly a five-fold increase in reported losses, equivalent to a compound annual growth rate of about 38 per cent, while complaint volumes grew by about 27 per cent over the same period; the average reported loss per complaint rose from about US\$5,300 to about US\$20,700 (Fig. 1a) [29,30]. With the exception of SIM-swap complaints, which declined slightly, the crime types most closely associated with unauthorised access and data acquisition were all higher in 2025 than in 2023 (Fig. 1b) [29]. These figures are victim-reported complaints rather than measures of offending, and IC3 crime types do not correspond to CFAA offence elements. They are presented only to show that the doctrinal questions examined here arise against a large and growing volume of incidents that must be classified, charged and located.

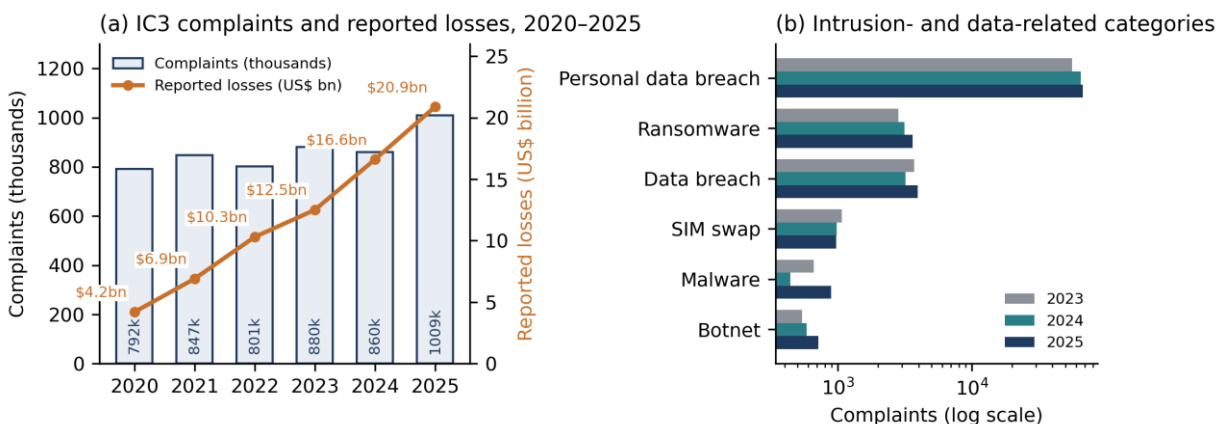


Fig. 1. Descriptive context: cyber-enabled crime reported to the FBI Internet Crime Complaint Center (IC3). (a) Annual complaints (bars) and reported losses (line), 2020–2025. (b) Complaint counts for intrusion- and data-related crime types, 2023–2025 (logarithmic scale). Source: compiled by the authors from IC3 annual reports [29,30]. Data are victim-reported, subject to under-reporting, and not aligned with statutory offence categories.

The United States Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, illustrates the first problem. Its principal access offences distinguish between access “without authorization” and access that “exceeds authorized access.” The Act defines the latter as accessing a computer with authorisation and using that access to obtain or alter information that the user is not entitled so to obtain or alter [1]. The statutory vocabulary seems simple, but decades of litigation have shown how difficult it is to distinguish hacking from misuse, disloyal conduct, credential sharing, policy violations and access after revocation. The Supreme Court’s decision in *Van Buren v United States* narrowed one branch of that debate by holding that a person who is entitled to obtain information from a computer does not “exceed authorised access” merely because the information is obtained for an improper purpose [2].

Van Buren did not, however, collapse all CFAA authorisation questions into a single rule. *United States v Nosal* addresses a different situation: access after an employer had affirmatively revoked the former employees' own credentials, followed by use of a current employee's credentials to reach the same proprietary system [3]. Read together, the cases suggest that cybercrime doctrine needs to keep purpose restrictions separate from permission boundaries. That distinction matters not only to criminal liability, but also to organisational design. A system may permit access technically while an organisation prohibits a use contractually; conversely, a user whose permission has been revoked may still find a technical route into the system. Legal authorisation and technical capability are related but not identical.

The second boundary problem is territorial. *United States v Auernheimer* concerned automated collection of AT&T customer email addresses through a web application weakness. The Third Circuit vacated the conviction because the essential conduct did not occur in New Jersey, notwithstanding that thousands of affected users were associated with that state [4]. *United States v Ivanov*, by contrast, concerned a Russian-based defendant accused of intruding into computers located in Connecticut and extorting a Connecticut business. The District Court rejected the argument that applying federal computer-crime statutes to the conduct amounted to an impermissible extraterritorial application, emphasising effects and protected interests within the United States [5]. The two cases illuminate distinct questions: *Auernheimer* is principally about constitutional and statutory venue within the United States; *Ivanov* is about the reach of United States law to conduct initiated abroad and causing effects in the forum.

This article brings these lines of authority together. Its central claim is that cybercrime disputes become clearer when analysed through two independent axes: an authorisation axis and a territorial-allocation axis. The authorisation axis asks whether the defendant crossed a permission boundary, an information-entitlement boundary, or merely a purpose-of-use restriction. The territorial axis asks which legally relevant locations are connected to the essential conduct, protected system, data, victim and effects, and whether the asserted forum is a valid place for adjudication rather than simply a place where consequences were felt.

The contribution is therefore not to argue that one case supplies a universal answer. Rather, the four cases demonstrate that "cyber boundary" disputes often involve different legal objects that are mistakenly treated as the same problem. *Van Buren* and *Nosal* are not inconsistent once improper purpose is separated from revoked permission. *Auernheimer* and *Ivanov* are not inconsistent once venue is separated from prescriptive jurisdiction and extraterritorial application. A structured framework based on those distinctions can improve doctrinal reasoning, charging decisions and cybersecurity governance.

The article proceeds as follows. Section 2 explains the doctrinal comparative method and the selection of the four cases. Section 3 sets out the statutory architecture of the CFAA and the conceptual difference between technical access, legal permission and information entitlement. Sections 4 and 5 analyse the authorisation and territorial lines of authority. Section 6 develops the two-axis digital-boundaries framework. Section 7 considers implications for organisational cybersecurity and investigation. Section 8 proposes legal and policy reforms. Section 9 identifies limitations, and Section 10 concludes.

2. Method and analytical contribution

This study uses a doctrinal legal method centred on primary authorities and supported by scholarship on computer authorisation and cybercrime jurisdiction. The analysis is comparative in the limited but important sense that it places four decisions dealing with different legal questions into a common conceptual matrix. The aim is not empirical measurement of cybercrime or prediction of judicial outcomes. It is to identify the legal variables that courts treat as decisive and to test whether those variables can be organised more coherently.

The four cases were selected because they expose two recurrent dimensions of cybercrime law. Van Buren and Nosal concern the meaning of authorisation under the CFAA but arise on opposite sides of an important factual line: improper use by a currently authorised user versus access following affirmative revocation. Auernheimer and Ivanov concern geographically distributed conduct but turn on different territorial doctrines: criminal venue in Auernheimer and extraterritorial/prescriptive reach in Ivanov. Each pair therefore permits a controlled comparison without pretending that the holdings answer identical questions.

Table 1 summarises the procedural profile of the four decisions. The set is deliberately heterogeneous in court and procedural posture—a Supreme Court merits decision, two courts of appeals decisions and a district court ruling on a motion to dismiss—because the aim is to test whether a single framework can organise holdings that arise at different stages and answer different legal questions. Both authorisation cases were decided by divided courts (6–3 and 2–1), which is itself an indicator of the interpretive difficulty the framework seeks to address.

Table 1. Procedural and factual profile of the four cases

Case	Court and year	Vote	Disposition	Legal question	Salient facts
Van Buren v United States [2]	US Supreme Court, 2021	6–3	Eleventh Circuit judgment reversed; remanded	Meaning of “exceeds authorized access”, § 1030(a)(2)	Police sergeant used his own valid credentials to run a licence-plate search in exchange for payment
United States v Nosal [3]	9th Cir., 2016	2–1	CFAA convictions affirmed	Access “without authorization” after revocation, § 1030(a)(4)	Former employees’ credentials revoked; a current employee’s password used to query a proprietary database
United States v Auernheimer [4]	3d Cir., 2014	3–0	Conviction vacated for improper venue	Criminal venue (Art. III; Sixth Amendment)	c. 114,000 email addresses collected; c. 4,500 (3.9%) linked to New Jersey residents; no essential conduct in New Jersey
United States v Ivanov [5]	D. Conn., 2001	Single judge	Motion to dismiss denied	Extraterritorial / prescriptive reach of US law	Defendant acting from Russia; intrusion into, and extortion of, a Connecticut business

Note: The earlier en banc decision in the same prosecution (Nosal I, 9th Cir. 2012, 9–2) held that “exceeds authorized access” concerns restrictions on access rather than on use [17]; Table 1 lists the 2016 panel decision (Nosal II), which addressed revocation. Sources: [2–5, 17].

The analysis also draws on literature that predates and follows Van Buren. Before the Supreme Court intervened, United States courts had divided over whether authorisation should be defined through duties and use restrictions or through a narrower, permission-based approach. Kane’s “available, granted, revoked” model is useful because it treats the existence and withdrawal of permission as separate stages [6]. Sacharoff similarly warns that the CFAA’s breadth cannot be solved by treating every computer-use norm as a criminal access rule [7]. Kerr’s analysis of Van Buren explains the Supreme Court’s focus on the locations or information a user is entitled to access rather than the user’s later purpose [8]. These accounts support a distinction between access boundaries and use restrictions, but the present article extends the analysis by connecting that distinction to territorial allocation.

On territoriality, the article relies on scholarship recognising that cyberspace complicates the localisation of conduct while not eliminating the legal importance of territory. Maillart argues that subjective territorial jurisdiction is difficult to apply when the place of cyber conduct is indeterminate [9]. Osula shows that cross-border access to data can raise separate questions of enforcement jurisdiction and sovereignty

[10]. De Hert, Parlar and Sajfert criticise unilateral expansion in access to electronic evidence and emphasise the need for clear international legal bases [11]. The Council of Europe's Budapest Convention and its Second Additional Protocol reflect the institutional response: cooperation mechanisms remain necessary precisely because digital evidence and providers are distributed across borders [12,13].

The article's analytical contribution is a two-axis framework. Axis A concerns access authorisation and contains five legally distinct states: (A1) public or generally available access; (A2) access granted to the user, with the information obtained falling within that grant; (A3) access granted to a system but not to a particular information area; (A4) access affirmatively revoked; and (A5) an access-controlled resource to which the actor never held permission, as in a conventional outsider intrusion. A separate variable records purpose restrictions because purpose alone does not necessarily change access status after Van Buren. Axis B concerns territorial allocation and records the location of the actor, the protected computer or server, the essential conduct, the data, the victim, and legally significant effects. For comparative purposes, the resulting territorial configuration can be summarised as (T1) single-forum, where actor, system and effects are co-located; (T2) distributed across several districts within one state; or (T3) cross-border, where the actor or key infrastructure is abroad. The framework then asks which territorial rule is being invoked: venue, prescriptive jurisdiction, adjudicative jurisdiction, or enforcement jurisdiction. This separation is the core of the article.

Fig. 2 locates the four cases on the resulting plane. Three features are apparent at the outset. First, the two authorisation cases share a territorial row but occupy different authorisation columns, so their different outcomes cannot be explained by geography. Second, the two territorial cases sit in different rows and turn on different doctrines, so their different outcomes cannot be explained by a single "cyber-jurisdiction" rule. Third, Auernheimer's position on the authorisation axis is marked as contested: because the Third Circuit decided the appeal on venue, it did not resolve whether collecting data from a public-facing endpoint crossed any access boundary [4].

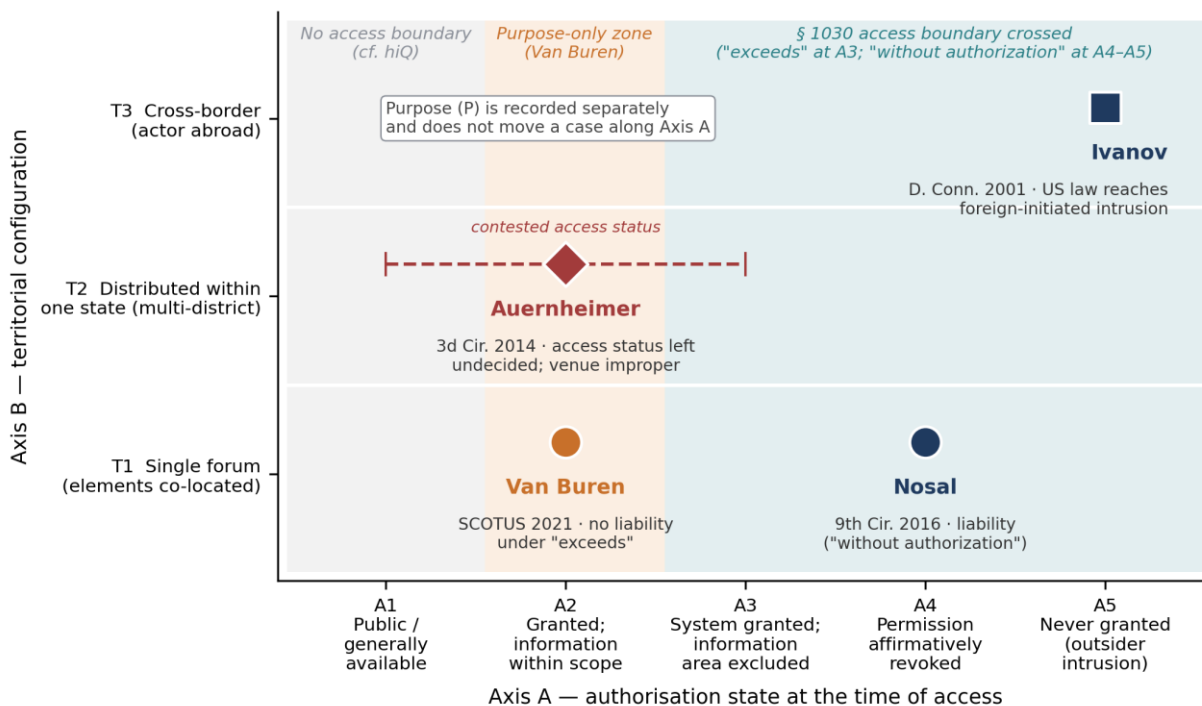


Fig. 2. The two-axis digital-boundaries framework, with the four cases located on it. Axis A records the authorisation state at the time of access (A1–A5); Axis B records the territorial configuration (T1–T3). Purpose is recorded separately and

does not move a case along Axis A. Auernheimer is shown as a range because its access status was not decided. Source: authors' analysis of [2–5,15].

3. The CFAA and the legal meaning of a computer boundary

3.1 Statutory architecture

The CFAA contains several offences, but its access language is central to disputes over insider misuse and credential-based intrusion. Section 1030(a)(2) prohibits intentionally accessing a computer without authorisation or exceeding authorised access and thereby obtaining specified categories of information, including information from a protected computer. Section 1030(a)(4) addresses knowing and fraudulent access to a protected computer without authorisation or by exceeding authorised access, coupled with furtherance of fraud and obtaining something of value. The statute defines “exceeds authorized access” in § 1030(e)(6) [1].

The statutory distinction creates two conceptual routes to liability. “Without authorization” ordinarily addresses a person who lacks permission to enter the relevant computer system. “Exceeds authorized access” addresses a person who has some permission to access the computer but obtains or alters information that lies outside the permitted scope. The difficulty is determining whether scope refers to information boundaries, use restrictions, contractual limits, purpose, or all of those things.

3.2 Technical capability is not the same as legal permission

A recurring mistake in cybercrime analysis is to equate what a computer technically permits with what the law authorises. Computers frequently accept valid credentials without evaluating the user's purpose. Websites may return information when an identifier is changed even though the operator did not intend to expose the information. Shared credentials can technically open a system after a particular person's own account has been disabled. These examples demonstrate that technical acceptance is evidentially relevant but not conclusive.

The reverse is also true. Legal permission does not mean that every use is desirable, ethical or contractually permitted. A police officer may be permitted to query a database for official purposes and still misuse information for personal gain. An employee may be permitted to retrieve a file but violate confidentiality rules by disclosing it. Treating every misuse as unauthorised computer access would transform private policies into potential triggers of federal criminal liability. This was one of the central concerns that drove narrow interpretations of the CFAA and ultimately informed Van Buren [2,8].

3.3 Information entitlement versus purpose restriction

Van Buren makes the distinction concrete. Nathan Van Buren was a police sergeant with valid credentials to a law-enforcement database. He accepted money to retrieve licence-plate information for an improper purpose. The government argued that he “exceeded authorized access” because departmental policy restricted the purposes for which he could use the database. The Supreme Court rejected that reading. It focused on whether Van Buren was entitled to obtain the particular information by using his authorised access. Because he was entitled to access the database and obtain that type of information, his improper motive did not convert the access into an “exceeds authorised access” violation [2].

The decision is often described through the “gates-up-or-down” metaphor. That shorthand is useful, but it should not obscure the statutory detail. The Court did not hold that policies never matter, that insider misuse is lawful, or that revocation is irrelevant. It held that the specific phrase “exceeds authorized access” is directed to obtaining information from areas or sources the user is not entitled to reach, rather than to misuse of information the user is otherwise entitled to obtain [2]. Other criminal, civil, disciplinary or employment rules may still regulate the misuse.

Van Buren also resolved a long-standing division among the federal courts of appeals (Fig. 3). Before 2021, the First, Fifth, Seventh and Eleventh Circuits had accepted broader readings under which contractual limits, duties of loyalty or purpose-based restrictions could render access unauthorised or excessive [31–34,37], whereas the Second, Fourth and Ninth Circuits had confined the statute to limits on access itself [17,35,36]. Within the Ninth Circuit, *LVRH Holdings v Brekka* had already tied authorisation to the employer’s grant of permission rather than to the employee’s loyalty [16], and the en banc decision in *Nosal* (*Nosal I*) held that “exceeds authorized access” concerns restrictions on access, not restrictions on use [17]. The Supreme Court’s 6–3 majority aligned with the narrower group [2]. It nevertheless left open whether the relevant limits must be technological (“code-based”) or may also be found in contracts or policies [2, n. 8]. That reservation is one reason why the framework developed below records the source of each boundary, and not merely its existence.

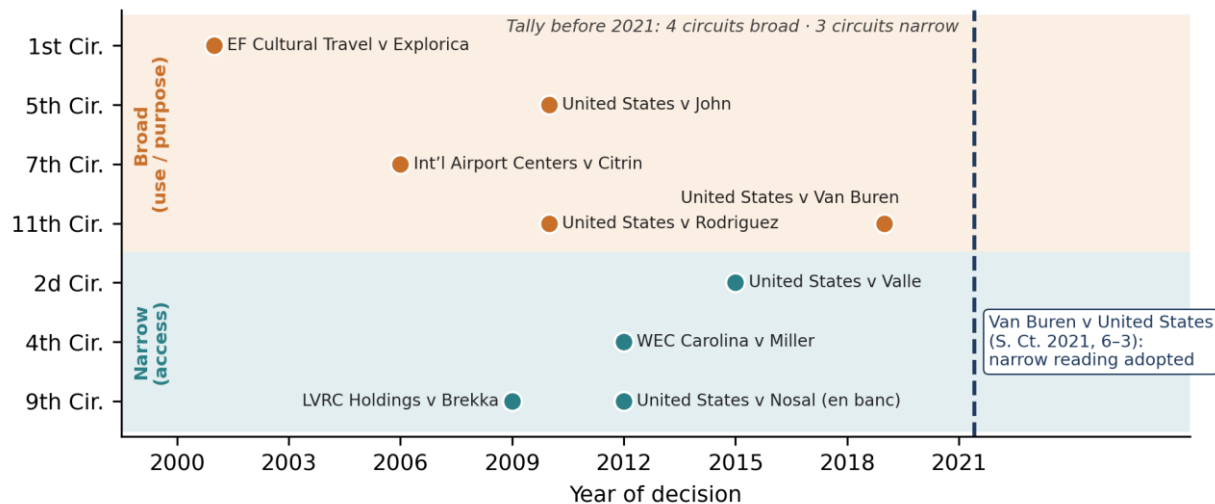


Fig. 3. The pre-Van Buren division among the federal courts of appeals on the scope of CFAA authorisation, 2001–2021. Each point marks a leading decision; shading indicates whether the circuit adopted a broad (use- or purpose-based) or narrow (access-based) reading. Before 2021 four circuits had adopted the broad reading and three the narrow reading. Sources: [2,16,17,31–37]; classification follows [2,8].

3.4 Revocation as a distinct legal event

Nosal illustrates why revocation belongs in a separate analytical category. After David Nosal and colleagues left Korn/Ferry, the company revoked their access credentials. They nevertheless obtained information from the proprietary Searcher database by using the credentials of a current employee. The Ninth Circuit held that once authorisation had been affirmatively rescinded, the former employees could not bypass the revocation by using another person’s credentials [3]. The court treated the conduct as access “without authorization,” not merely as a violation of a purpose restriction.

This distinction survives *Van Buren*. *Van Buren* involved a user whose own credentials were valid and whose access extended to the information obtained. *Nosal* involved former users whose permission had been affirmatively revoked. The two cases therefore occupy different cells in an authorisation matrix. *Van Buren* limits purpose-based expansion of “exceeds authorised access”; *Nosal* addresses circumvention of a permission withdrawal under the “without authorization” branch.

3.5 Why the distinction matters for legality

The criminal law principle of legality requires offences to provide fair notice and to avoid arbitrary expansion. If “authorisation” were defined entirely by private computer-use policies, criminal exposure could vary with employer handbooks, website terms or informal instructions. Scholars have long warned that this could

federalise ordinary workplace misconduct or contractual breach [6–8,14]. A permission-centred approach does not solve every ambiguity, but it creates a more administrable boundary: whether the defendant had permission to enter the relevant system or information area, and whether that permission remained in force.

At the same time, a purely technical conception would be too narrow. Revoked users may retain cached credentials or obtain another user's password. Attackers may exploit an interface that responds without an explicit access-control check. The law therefore requires evidence of permission and entitlement rather than mere proof that the system responded. The practical challenge is to identify the relevant legal boundary without treating every system weakness as consent.

4. The authorisation axis: Van Buren and Nosal

4.1 Van Buren: misuse within a granted access domain

The core fact in Van Buren was that the defendant did not need to defeat a technical barrier to obtain the licence-plate record. He used valid credentials and accessed a database available to him as a police officer. His wrongdoing lay in the purpose for which he performed the search: personal financial benefit rather than legitimate police work. The Supreme Court's majority read § 1030(e)(6) as asking whether the user was entitled to obtain the information in the manner relevant to the statutory definition, not whether the user had a proper downstream reason for obtaining it [2].

This interpretation narrows the CFAA's role as an insider-misuse statute. It reduces the risk that ordinary violations of acceptable-use policies become federal crimes. That is a significant rule-of-law benefit. Criminal liability becomes less dependent on contractual drafting and organisational policy detail. The decision also preserves conceptual space for other legal regimes—bribery law, trade-secret law, privacy rules, fiduciary duties, employment sanctions and sector-specific confidentiality obligations—to address misuse that is not hacking.

The limit of the decision is equally important. A narrow access offence does not eliminate insider risk. Organisations still need to control legitimate users who may misuse privileges. The legal boundary and the security boundary therefore diverge. Role-based access control, logging, anomaly detection and segregation of duties may be necessary even when the user's access remains legally authorised. Cybersecurity governance cannot assume that the criminal law will convert every improper query into a CFAA offence.

4.2 Nosal: access after permission has been withdrawn

Nosal presents a structurally different problem. Korn/Ferry disabled the former employees' own credentials. The former employees then relied on the password of a current employee to enter the company's proprietary system. The Ninth Circuit treated affirmative revocation as decisive: when the system owner has rescinded a person's permission, that person cannot restore authorisation through a third party who remains authorised [3].

The 2–1 majority's reasoning was controversial because password sharing can occur in benign contexts. Judge Reinhardt's dissent warned that an expansive reading might threaten innocuous conduct. The majority responded by emphasising the specific facts: access to a proprietary internal database, affirmative revocation, circumvention, and fraudulent purpose [3]. This factual specificity should be retained when using Nosal as a precedent. The case is strongest as authority for the proposition that an owner's clear withdrawal of permission has legal significance; it is weaker as a general rule that every act of credential sharing is criminal.

4.3 A reconciled reading

The apparent tension between Van Buren and Nosal largely disappears once three variables are separated:

First, who granted access? Van Buren had direct institutional credentials and continuing permission to use the database. In Nosal, the relevant users' direct permission had been withdrawn.

Second, what information was within the granted access domain? Van Buren obtained information of a type available to him through his authorised account. Nosal's former employees no longer had a granted domain at all.

Third, what role does purpose play? In Van Buren, improper purpose alone was insufficient to establish "exceeds authorised access." In Nosal, purpose was not the only boundary; the defendants confronted an affirmative revocation of access.

The cases therefore support a rule that may be expressed as follows: purpose restrictions should generally be analysed separately from access permission, while affirmative revocation changes the permission state. This rule is compatible with the statutory distinction between "exceeds authorized access" and "without authorization" and avoids collapsing disloyalty, confidentiality and computer trespass into a single offence.

4.4 The unresolved edge cases

Important questions remain. Public websites do not fit comfortably into an employee-access model. Technical barriers can be ambiguous: a rate limit, robots exclusion instruction, IP block or cease-and-desist notice may communicate different kinds of restriction. Data-scraping litigation has shown that courts must distinguish publicly available information from restricted computer areas and must determine when a barrier represents legally effective revocation [15]. Van Buren does not answer all of those questions.

Another unresolved issue is machine-to-machine access. Automated agents, APIs and service accounts may act under delegated credentials. In such settings, the relevant "user" may be a person, organisation, application or combination of actors. The proposed framework therefore treats authorisation as a relation among a principal, credential, protected resource and time. It asks what permission existed at the moment of access and what specific information boundary the permission covered.

5. The territorial axis: Auernheimer and Ivanov

5.1 Why cybercrime cannot be located by harm alone

Cyber incidents generate multiple candidate locations. The person initiating a request may be in one state; the web server may be in another; the database may be replicated across several regions; users may be distributed nationally; and financial or privacy harms may arise wherever victims live. If each location were automatically sufficient for every jurisdictional purpose, cybercrime could be prosecuted almost anywhere. That would undermine venue protections and create substantial forum-selection power for prosecutors.

The law therefore distinguishes different territorial questions. Prescriptive jurisdiction concerns a state's authority to make law applicable to conduct. Adjudicative jurisdiction concerns the authority of courts to hear disputes. Enforcement jurisdiction concerns coercive acts taken to investigate or enforce law, especially across borders. Venue determines the proper geographic place of trial within the relevant judicial system. These doctrines can overlap factually but they are not interchangeable [9–11]. Brenner and Koops's survey of approaches to cybercrime jurisdiction shows that territorial, effects-based and nationality-based claims frequently overlap, so that the practical problem is more often competing jurisdiction than an absence of it [26].

5.2 Auernheimer: venue and essential conduct

Auernheimer arose from a weakness in AT&T's web-based system for iPad users. By manipulating an identifier, requests could cause the system to reveal associated email addresses. Daniel Spitler created an automated process that collected a large number of addresses; Andrew Auernheimer participated in the project and publicised the vulnerability. At the relevant time Spitler was in San Francisco, Auernheimer was in Fayetteville, Arkansas, and AT&T's servers were located in Dallas and Atlanta. Of the approximately 114,000 email addresses collected, around 4,500—roughly 3.9 per cent—belonged to New Jersey residents [4].

The Third Circuit vacated Auernheimer's conviction because venue was improper in New Jersey. Venue in federal criminal cases rests on Article III and the Sixth Amendment [22], and the Supreme Court has directed courts to identify the essential conduct elements of the charged offence and then determine where those elements were committed [24,25]. Applying that approach, the court found that neither Auernheimer nor Spitler performed any essential conduct element of the CFAA or identity-fraud charges, or any overt act in furtherance of the conspiracy, in New Jersey. It treated the location of effects, standing alone, as insufficient, and emphasised that venue is a constitutional safeguard, not a technical convenience [4]. The continuing-offence provision in 18 U.S.C. § 3237(a), which permits prosecution of an offence begun in one district and completed in another in any district in which it was begun, continued or completed [23], rests on the same logic of locating conduct rather than consequences. This is especially significant in cybercrime because distributed consequences could otherwise make virtually any affected district a permissible prosecution venue.

Auernheimer therefore stands for a restraint principle: downstream effects and victim residence do not automatically locate the essential conduct of an offence. Prosecutors must identify the conduct elements and connect them to the proposed venue. The case does not establish that the underlying data collection was lawful, nor does it resolve every CFAA question. Its precedential force is territorial and procedural.

5.3 Ivanov: foreign conduct and domestic effects

Ivanov addresses a different problem. Aleksey Ivanov, operating from Russia, was accused of intruding into computers belonging to Online Information Bureau in Connecticut, obtaining data and using the intrusion as part of an extortion scheme. He challenged the application of United States law on the ground that he had acted from Russia. The District Court rejected the challenge, reasoning that the charged conduct was directed at and produced effects within the United States and that the relevant statutory scheme could reach the conduct alleged [5]. The court also read the 1996 amendments to the CFAA, including the statute's reference to computers used in interstate or foreign commerce and the accompanying legislative history, as indicating that Congress intended the Act to reach intrusions launched from abroad [5]. Congress subsequently extended the statute's territorial reach in the other direction: the USA PATRIOT Act amended the definition of "protected computer" in § 1030(e)(2)(B) to include a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States [1,39]. The combined effect is that the CFAA can reach both foreign actors who attack domestic systems and, in defined circumstances, attacks on foreign systems that affect United States commerce.

The case demonstrates why location of the actor cannot be the only jurisdictional fact in cybercrime. A remote intrusion can directly manipulate a protected computer situated in the forum. Where the protected system, data and economic target are located domestically, a state has a stronger territorial connection than in a case based only on diffuse victim effects. Ivanov is therefore best understood as an example of objective territoriality/effects reasoning applied to conduct initiated abroad.

The practical enforcement story is more complicated. Legal authority to prescribe or adjudicate does not itself place a foreign defendant before the court. Ivanov's apprehension depended on an undercover operation that brought him to the United States. Cross-border cybercrime thus separates normative jurisdiction from enforcement capacity. International cooperation, extradition, mutual legal assistance and evidence-sharing mechanisms remain necessary even where the forum has a plausible substantive jurisdictional claim.

5.4 Venue is not the same as extraterritorial jurisdiction

Placing Auernheimer and Ivanov side by side reveals why cybercrime analysis often becomes confused. Both cases involve distributed geography, but they ask different questions. In Auernheimer, the United States plainly had criminal law and courts capable of hearing a CFAA prosecution; the issue was which federal district was a constitutionally proper venue. In Ivanov, the challenge concerned the application of United States law to conduct initiated outside the country and causing domestic effects.

A broad effects doctrine cannot cure a defective venue. Conversely, a narrow venue holding does not necessarily limit the national substantive reach of the statute. The territorial axis must therefore identify the legal doctrine before evaluating the factual nexus. This is a central part of the two-axis framework developed below.

Fig. 4 makes the contrast concrete by mapping each legally relevant location against the forum asserted by the prosecution. In Auernheimer, every conduct-related location—the actors, the servers and the place where the data were obtained—lay outside New Jersey, and the forum connection rested entirely on victims and effects, which accounted for only about 3.9 per cent of the affected users. In Ivanov, by contrast, the protected computer, the data and the targeted business were all in the forum, and only the actor was abroad. The comparison shows why counting connections is not enough: what matters is which locations are relevant to the doctrine invoked. For venue, conduct locations are decisive; for prescriptive reach, the location of the protected system and of intended effects can carry substantial weight.

(a) Territorial map		Auernheimer forum: D. New Jersey · issue: venue	Ivanov forum: United States (D. Conn.) · issue: reach
Actor(s) at time of conduct	Outside	Spitler: San Francisco, CA Auernheimer: Fayetteville, AR	Outside Russia
Protected computer / server	Outside	AT&T servers: Dallas, TX and Atlanta, GA	In forum Online Information Bureau, Vernon, Connecticut
Data obtained	Outside	Retrieved from AT&T servers outside NJ	In forum Victim's data held on Connecticut computers
Essential conduct elements	Outside	No essential conduct element in NJ	Partly Initiated abroad; intrusion executed on forum computers
Victims	Partly	c. 4,500 of 114,000 addresses (3.9%) in NJ	In forum Connecticut business
Harmful effects	Partly	Diffuse; partly felt by NJ residents	In forum Extortion demands and harm directed at forum
Outcome		Venue improper; conviction vacated	US law applies; dismissal denied

(b) Auernheimer: residence of affected iPad users (email addresses obtained)

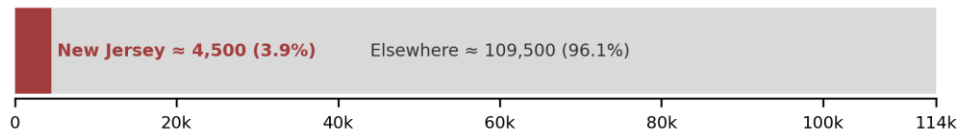


Fig. 4. Territorial mapping of Auernheimer and Ivanov. (a) Location of each legally relevant element relative to the forum asserted by the prosecution. (b) Share of affected users associated with New Jersey in Auernheimer (approximately 4,500 of 114,000 email addresses). Sources: [4,5]; authors' analysis.

5.5 Cross-border evidence and sovereignty

Modern cyber investigations also require access to electronic evidence held by providers or systems in other countries. That raises enforcement-jurisdiction and sovereignty issues separate from the place of trial. Osula argues that unilateral transborder access may amount to extraterritorial enforcement and therefore requires an explicit legal basis to avoid breaching sovereignty [10]. De Hert, Parlar and Sajfert similarly caution against using flexible interpretation to bypass formal inter-state agreement [11].

The Budapest Convention responds through cooperative obligations and jurisdictional rules, while the Second Additional Protocol introduces additional mechanisms for disclosure of electronic evidence and direct cooperation with service providers subject to safeguards [12,13]. These instruments do not eliminate territoriality. They confirm its continuing importance by creating legal pathways for cooperation when evidence and providers sit outside the investigating state.

Other instruments illustrate the same point. The United States CLOUD Act of 2018 addressed provider disclosure of data stored abroad and created a framework for bilateral executive agreements, a development Daskal describes as a new mode of international lawmaking operating through domestic legislation and bilateral arrangements [20]. Within the European Union, the Council authorised member states in April 2022 to sign the Second Additional Protocol in the interest of the Union [21]. These mechanisms respond to well-

documented weaknesses of traditional mutual legal assistance, which is slow and poorly adapted to volatile, cloud-hosted evidence [27,28]. The cross-border dimension is visible even in domestic complaint data: IC3 received complaints from more than 200 countries in 2025, associated with almost US\$1.6 billion of reported losses [29].

6. A two-axis digital-boundaries framework

6.1 Overview

The four cases can be organised into a two-axis framework designed to prevent analytical category errors. The first axis is authorisation. The second is territorial allocation. Each axis contains questions that should be answered independently before they are combined.

The authorisation axis asks:

- (1) Is the relevant computer or information publicly available or access-controlled?
- (2) Did the defendant have direct permission to access the computer?
- (3) If yes, did that permission extend to the specific information or computer area obtained?
- (4) Had permission been affirmatively revoked before the access?
- (5) Was the alleged wrong only an improper purpose or downstream misuse?
- (6) Were third-party credentials, technical circumvention or automation used, and what do those facts show about permission?

The territorial axis asks:

- (1) Where was the actor when the essential conduct occurred?
- (2) Where was the protected computer or server?
- (3) Where was the relevant data stored or obtained?
- (4) Where did the essential conduct element occur, as distinct from downstream harm?
- (5) Where were victims located and where were legally significant effects felt?
- (6) Which territorial doctrine is being invoked: venue, prescriptive jurisdiction, adjudicative jurisdiction or enforcement jurisdiction?
- (7) Does exercising that authority require cross-border investigative or coercive action?

6.2 Comparative case matrix

Table 2 applies the framework to the four cases, and Fig. 2 locates the same cases graphically. The value of the matrix is not that it mechanically decides liability. It makes explicit which boundary the court was actually deciding.

Van Buren occupies the “permission granted / information within entitlement / improper purpose” cell. Nosal occupies the “permission revoked / alternate credentials used” cell. Auernheimer occupies the “distributed conduct / victim effects in proposed venue but essential conduct elsewhere” cell. Ivanov occupies the “actor abroad / protected system and effects in forum” cell.

Table 2. Application of the two-axis digital-boundaries framework

Case	Access/authorisation state	Territorial configuration	Primary legal question	Doctrinal lesson
Van Buren	A2 – Own valid credentials; information within granted access; improper purpose	T1 – Domestic	Meaning of “exceeds authorised access”	Purpose restriction is not automatically an access boundary

Nosal	A4 – Own access affirmatively revoked; current employee's credentials used	T1 – Domestic	Meaning of access "without authorization" after revocation	Revocation changes the permission state; circumvention can be decisive
Auernheimer	A1/A3 (contested) – Public-facing application weakness; automated data collection	T2 – Actors/servers outside New Jersey; some affected users in New Jersey	Criminal venue	Victim effects alone do not necessarily locate essential conduct
Ivanov	A5 – Unauthorised remote intrusion	T3 – Actor in Russia; protected system/business in Connecticut	Extraterritorial/prescriptive reach	Foreign initiation does not eliminate a substantial domestic territorial nexus

6.3 The non-substitution principle

The framework produces a broader doctrinal principle: one boundary cannot substitute for another. Strong evidence of improper purpose cannot substitute for proof that a CFAA access boundary was crossed. Serious victim harm in a district cannot substitute for constitutionally proper venue where the offence's essential conduct occurred elsewhere. A plausible national jurisdictional basis cannot substitute for lawful cross-border enforcement measures. Technical accessibility cannot automatically substitute for legal permission, and technical blocking cannot by itself resolve every question of legal authorisation.

This non-substitution principle has practical value. It encourages prosecutors to charge offences according to the legal wrong actually established, rather than stretching access concepts to capture misuse. It encourages courts to identify the precise territorial doctrine at issue. It also encourages organisations to design controls around risks that criminal law may not reach.

6.4 Temporal state matters

Authorisation is not static. Nosal shows that access can move from granted to revoked. Employment termination, account suspension, privilege changes, role transfer and contract expiry can all change the legal and technical state. A sound analysis must therefore identify the time of the disputed access. Evidence of clear revocation—account disablement, notice, access-control logs and de-provisioning records—can be legally significant.

Territorial facts can also change over time. Cloud systems migrate data, route traffic dynamically and replicate information. For venue and jurisdiction, courts should focus on legally relevant acts rather than assuming that every transient network hop creates a forum. Otherwise, infrastructure architecture could produce arbitrary criminal geography.

6.5 Purpose as an independent variable

After Van Buren, purpose should be recorded but not automatically treated as an access boundary under § 1030(e)(6). Improper purpose may establish mens rea for another offence, support bribery, fraud or trade-secret charges, or justify organisational discipline. It may also provide context for interpreting ambiguous conduct. But treating purpose as a substitute for information entitlement risks recreating the overbreadth the Supreme Court rejected.

This separation creates a more principled relationship between cybercrime law and cybersecurity governance. The criminal law can focus on computer trespass and clearly defined access violations, while organisations regulate broader misuse through policy, monitoring and sectoral obligations.

6.6 Applying the framework as a structured legal test

For practical use, the framework can be expressed as a sequential test (Fig. 5). A court or investigator should first define the protected resource with precision: the computer, account, database, application endpoint or information area allegedly crossed. General descriptions such as “the company network” are often too imprecise because a user may be entitled to some resources but excluded from others. The second step is to identify the source of permission and its status at the time of access. Relevant evidence may include account provisioning records, role assignments, contractual terms, revocation notices and technical logs. The third step is to separate information entitlement from purpose. If the defendant could obtain the same information through the granted access path, an improper motive should not automatically be recharacterised as exceeding access after *Van Buren*. If access had been affirmatively withdrawn, Nosal indicates that use of another person’s credentials may instead support a “without authorization” theory.

The territorial test should then begin with the offence’s essential conduct elements rather than with a map of all consequences. Investigators should identify where the acts constituting access, acquisition, transmission, damage, extortion or other charged conduct occurred. Only after that should victim location and harmful effects be added. This ordering matters because a cyber incident may have thousands of victims in many districts, while the acts that legally constitute the offence occurred in only a few places. Auernheimer demonstrates the procedural risk of starting from affected users and working backward to venue.

For cross-border cases, a final layer should distinguish the state’s claim to apply its substantive law from the means used to obtain evidence or custody. A forum may have a substantial territorial connection because a protected computer was located within it, as in *Ivanov*, yet investigators may still need consent, treaty-based assistance, provider cooperation or extradition to act outside national territory. Treating those stages separately prevents a valid substantive-jurisdiction argument from becoming an implicit licence for extraterritorial enforcement.

The structured test also assists defence analysis and judicial review. It requires the prosecution to identify the exact boundary allegedly crossed and the exact territorial rule relied upon. That improves notice and makes overbreadth easier to detect. In policy terms, the approach favours narrower, fact-specific criminalisation supported by complementary privacy, employment, trade-secret and cybersecurity regimes rather than asking the CFAA to perform every regulatory function associated with misuse of digital information.

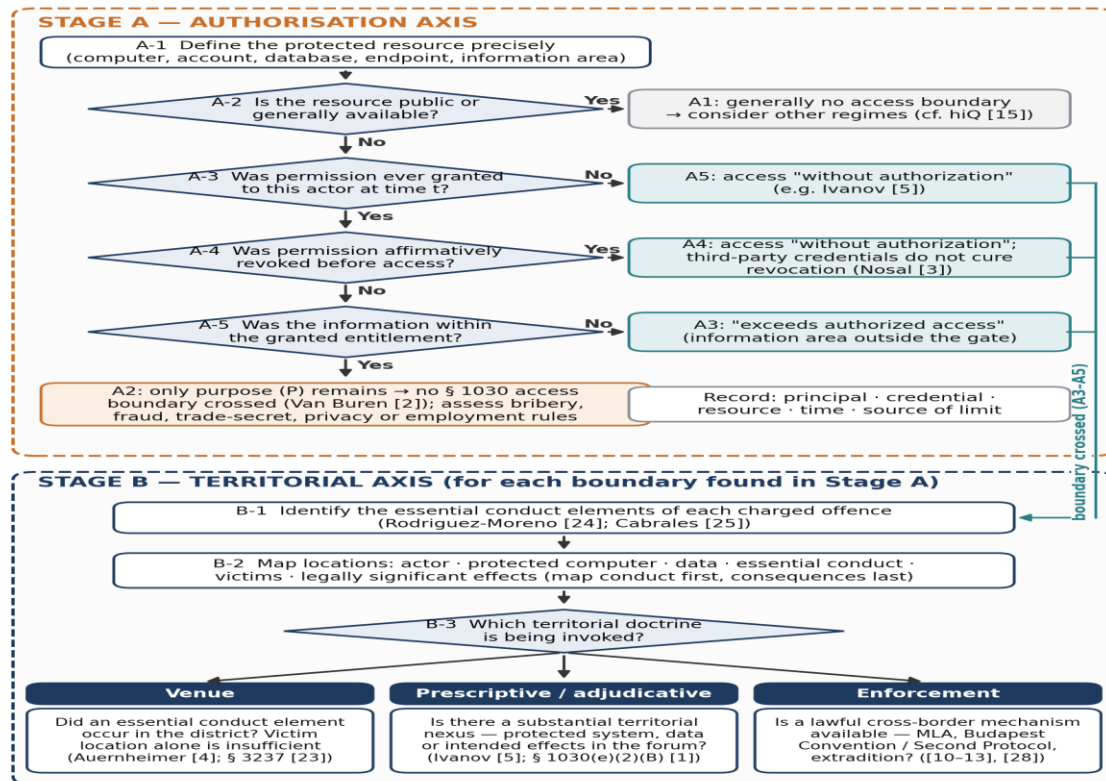


Fig. 5. Structured decision model for applying the two-axis framework. Stage A classifies the authorisation state at the time of access; Stage B is applied to each boundary identified and requires the territorial doctrine to be named before the factual nexus is assessed. Source: authors' analysis.

7. Implications for cybersecurity governance and investigation

7.1 Access control should make legal boundaries observable

The legal analysis has a direct governance implication: organisations should make permission boundaries explicit and technically enforceable where possible. Least privilege, role-based access control and timely de-provisioning reduce attack surface, but they also generate clearer evidence of who was entitled to access which resources. If permissions are vague, shared or retained long after a role changes, both security and legal attribution become more difficult.

Van Buren is a reminder that a user may lawfully possess access rights while acting for an improper purpose. Monitoring therefore remains necessary. Database audit logs, behavioural alerts, separation of duties and approval workflows can identify suspicious use without pretending that the user lacked all authorisation. Legal classification and risk management can thus remain distinct.

Nosal highlights the importance of revocation. Termination or role-change processes should disable accounts promptly, rotate shared secrets and revoke tokens. Organisations should also avoid generic shared credentials. Unique identities and multi-factor authentication improve both security and evidentiary clarity. Where the organisation has unequivocally withdrawn permission, continued access is easier to distinguish from a mere policy dispute.

These controls can also be understood through routine activity theory, which explains crime as the convergence of a motivated offender and a suitable target in the absence of a capable guardian [18]. Empirical work applying the theory to cybercrime suggests that its elements translate unevenly to online settings, with target visibility

proving more consistently relevant than some forms of technical guardianship [19]. The legal analysis adds a further dimension: least privilege, prompt de-provisioning and logging act not only as guardianship that reduces opportunity, but also as the evidential record that later allows a court to determine which authorisation state (A1–A5) applied at the time of access.

7.2 Public-facing systems and responsible disclosure

Auernheimer illustrates a different governance problem: public-facing systems may unintentionally reveal information when inputs are manipulated or identifiers are enumerated. Organisations should not rely on obscurity or assumptions about normal user behaviour. Input validation, access-control checks on every request, rate limiting, logging and privacy-by-design controls are relevant. Responsible-disclosure programmes can also reduce incentives for researchers to collect unnecessary personal data when demonstrating a vulnerability.

The legal framework should likewise avoid conflating research, scraping and harmful intrusion. The key question should be what access boundary existed and what information the actor was entitled to obtain, not simply whether automation was used. Automation changes scale and risk, but not by itself the legal status of every request. Prosecutorial policy has moved in the same direction: in May 2022 the United States Department of Justice revised its CFAA charging policy to direct that good-faith security research should not be charged under the Act [38].

7.3 Investigative territorial mapping

Investigators should create a territorial map early in a cybercrime inquiry. The map should distinguish actor location, protected-computer location, data location, victim location, provider location and places where essential conduct occurred. The map should then be matched to the specific doctrine relevant to charging and evidence acquisition.

This practice would have obvious value in an Auernheimer-type case because it forces the prosecution to identify the district connected to the conduct elements before indictment. In an Ivanov-type case, the same map clarifies the basis for national jurisdiction while exposing the separate need for lawful cross-border evidence gathering and apprehension. Fig. 4 illustrates the form such a map can take.

7.4 International cooperation rather than jurisdictional improvisation

Cybercrime creates pressure for fast access to evidence, but speed should not erase sovereignty and due-process constraints. International instruments increasingly provide mechanisms for direct provider cooperation, emergency assistance and production of electronic evidence [12,13]. Those mechanisms should be used where applicable rather than relying on unilateral investigative acts with uncertain legal foundations.

The policy direction is therefore not a borderless criminal law. It is a better-connected system of bounded authorities. States can maintain territorial and procedural safeguards while improving interoperability, standardising requests and accelerating preservation and disclosure.

8. Legal and policy recommendations

The analysis supports six reforms.

First, legislatures should preserve a clear distinction between unauthorised access and unauthorised use. Criminal access offences should focus on crossing permission or information-entitlement boundaries. If misuse of lawfully accessed data requires additional criminalisation, it should be addressed through specifically defined offences rather than by expanding “access” beyond recognition.

Second, organisations and statutes should give affirmative revocation a clear legal and evidentiary role. Revocation should be communicated and technically implemented. In contested cases, courts should examine whether the system owner clearly withdrew the defendant's permission before the access occurred.

Third, venue rules for cybercrime should continue to focus on essential conduct rather than victim location alone. Distributed harms can be relevant, but they should not become a universal venue hook. Legislatures may clarify cyber-specific venue where constitutionally permissible, but any reform should retain a meaningful connection between the forum and the conduct charged.

Fourth, courts should identify the territorial doctrine explicitly. "Jurisdiction" is too broad a label. A judgment should distinguish prescriptive reach, adjudicative authority, venue and enforcement jurisdiction. This would prevent reasoning from one category being imported into another without analysis.

Fifth, cross-border investigative powers should rest on explicit legal bases and safeguards. The Budapest Convention and Second Additional Protocol demonstrate a cooperative approach to electronic evidence [12,13]. States should continue to improve speed and standardisation while protecting privacy, due process and sovereignty.

Sixth, prosecutors should use a boundary checklist at charging stage. For a CFAA access count, the file should identify the permission source, resource, information entitlement, revocation status and alleged circumvention. For a geographically distributed offence, the file should identify the essential conduct and explain the territorial basis for the selected venue and any extraterritorial application. Such documentation would improve consistency and reduce the risk of overbroad charging.

9. Limitations

This article is doctrinal and case-centred. It does not provide empirical evidence about charging practices, conviction rates or organisational security outcomes. The IC3 statistics in Fig. 1 are descriptive context only. They are victim-reported complaints subject to substantial under-reporting—the FBI has noted that when it infiltrated the Hive ransomware group, only about 20 per cent of the group's victims had reported to law enforcement [30]—and IC3 crime types are not defined by reference to CFAA offence elements. They cannot therefore be used to estimate how many incidents fall into any authorisation state or territorial configuration identified here. Linking the framework to case-level charging and sentencing data would be a valuable direction for future empirical work. The four cases are United States authorities, although the territorial discussion draws on international cybercrime scholarship and the Budapest Convention. Comparative work involving the United Kingdom, Australia, the European Union and additional national computer-misuse regimes could test whether the framework travels across statutory systems.

The cases also span different technological periods. Ivanov predates contemporary cloud computing and global platform infrastructure, while Van Buren reflects a more mature debate about access controls and data use. That temporal variation is a limitation, but it also demonstrates the persistence of the underlying boundary problems.

Finally, the framework simplifies facts that may be contested in real litigation. Whether a user was "entitled" to information can depend on system architecture, contract, policy, code and organisational practice. Data location may be dynamic. The framework is therefore intended as a disciplined sequence of questions, not an algorithm that eliminates judicial interpretation.

10. Conclusion

Cybercrime law does not fail because cyberspace has no boundaries. It struggles because digital activity creates several different boundaries at once. The CFAA distinguishes entry without permission from obtaining information beyond an authorised scope. Organisations impose purpose restrictions that may not coincide with criminal access rules. Networks distribute actors, servers, data, victims and effects across multiple places. Criminal procedure then asks which of those places matters for venue, jurisdiction and enforcement.

Van Buren and Nosal show why improper purpose should not be confused with revoked permission. Van Buren limits the use of the CFAA to criminalise misuse of information a person is otherwise entitled to obtain; Nosal confirms the significance of affirmative revocation and circumvention. Auernheimer and Ivanov show why victim effects should not be confused with every territorial doctrine. Auernheimer protects the constitutional significance of venue by requiring a proper connection to essential conduct. Ivanov demonstrates that conduct initiated abroad may still have a substantial domestic jurisdictional nexus when protected systems and harmful effects are located in the forum.

The two-axis digital-boundaries framework developed here turns those lessons into a structured method. On the authorisation axis, decision-makers should identify permission, information entitlement, revocation and purpose separately. On the territorial axis, they should map actor, system, data, conduct, victim and effects and then identify whether the issue is venue, prescriptive jurisdiction, adjudicative authority or enforcement. The non-substitution principle follows: evidence relevant to one boundary should not automatically replace proof required for another.

For policymakers, the result is a case for precise offences, clear revocation rules, conduct-based venue, and formal cross-border cooperation. For organisations, it is a case for least privilege, strong de-provisioning, logging and responsible disclosure. For courts and investigators, it is a case for naming the boundary before deciding whether it was crossed. That approach can make cybercrime law both more effective and more legally restrained.

Declarations

Funding: No external funding was used for this doctrinal study.

Declaration of competing interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability: No new datasets were generated. The study is based on publicly available legislation, judicial decisions and published literature. Fig. 1 uses publicly available aggregate statistics from the FBI Internet Crime Complaint Center annual reports [29,30]; case-level figures in Table 1 and Fig. 4 are taken from the cited judicial decisions.

Ethics: Ethics approval was not required because the study did not involve human participants, personal data collection, or experiments.

References

- [1] 18 U.S.C. § 1030, Fraud and related activity in connection with computers.
- [2] Van Buren v. United States, 593 U.S. 374 (2021).
- [3] United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016).
- [4] United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014).

- [5] United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001).
- [6] S. Kane, Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act, *Univ. Chic. Law Rev.* 87 (2020) 1437–1494.
- [7] L. Sacharoff, Criminal Trespass and Computer Crime, *William & Mary Law Rev.* 62 (2020) 571–646.
- [8] O.S. Kerr, Focusing the CFAA in Van Buren, *Supreme Court Rev.* 2021 (2022) 155–184. <https://doi.org/10.1086/720376>.
- [9] J.-B. Maillart, The limits of subjective territorial jurisdiction in the context of cybercrime, *ERA Forum* 19 (2019) 375–390. <https://doi.org/10.1007/s12027-018-0527-2>.
- [10] A.-M. Osula, Transborder access and territorial sovereignty, *Comput. Law Secur. Rev.* 31 (2015) 719–735. <https://doi.org/10.1016/j.clsr.2015.08.003>.
- [11] P. De Hert, C. Parlar, J. Sajfert, The Cybercrime Convention Committee’s 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law, *Comput. Law Secur. Rev.* 34 (2018) 327–336. <https://doi.org/10.1016/j.clsr.2018.01.003>.
- [12] Council of Europe, Convention on Cybercrime (ETS No. 185), Budapest, 23 November 2001.
- [13] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), 2022.
- [14] T.E. Booms, Hacking into Federal Court: Employee “Authorization” Under the Computer Fraud and Abuse Act, *Vanderbilt J. Ent. & Tech. Law* 13 (2011) 543–588.
- [15] *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022).
- [16] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009).
- [17] *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc).
- [18] L.E. Cohen, M. Felson, Social change and crime rate trends: A routine activity approach, *Am. Sociol. Rev.* 44 (1979) 588–608. <https://doi.org/10.2307/2094589>.
- [19] E.R. Leukfeldt, M. Yar, Applying routine activity theory to cybercrime: A theoretical and empirical analysis, *Deviant Behav.* 37 (2016) 263–280.
- [20] J. Daskal, Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0, *Stanford Law Rev. Online* 71 (2018) 9–16.
- [21] Council of the European Union, Access to e-evidence: Council authorises member states to sign international agreement, 5 April 2022.
- [22] United States Constitution, Art. III, § 2, cl. 3; amend. VI.
- [23] 18 U.S.C. § 3237, Offenses begun in one district and completed in another.
- [24] *United States v. Rodriguez-Moreno*, 526 U.S. 275 (1999).
- [25] *United States v. Cabrales*, 524 U.S. 1 (1998).
- [26] S. Brenner, B.-J. Koops, Approaches to cybercrime jurisdiction, *J. High Tech. Law* 4 (2004) 1–46.
- [27] B.-J. Koops, M. Goodwin, Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law, *Tilburg Institute for Law, Technology, and Society*, 2014.
- [28] A.-M. Osula, Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data, *Masaryk Univ. J. Law Tech.* 9 (2015) 43–64.
- [29] Federal Bureau of Investigation, Internet Crime Complaint Center, 2025 IC3 Annual Report (Internet Crime Report), Washington, DC, 2026. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

- [30] Federal Bureau of Investigation, Internet Crime Complaint Center, Internet Crime Report 2023, Washington, DC, 2024. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.
- [31] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).
- [32] International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).
- [33] United States v. John, 597 F.3d 263 (5th Cir. 2010).
- [34] United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).
- [35] WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).
- [36] United States v. Valle, 807 F.3d 508 (2d Cir. 2015).
- [37] United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019).
- [38] United States Department of Justice, Justice Manual § 9-48.000, Computer Fraud and Abuse Act (charging policy revised 19 May 2022).
- [39] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 814, 115 Stat. 272.