
SUPREME COURT OF THE UNITED STATES —
CHAMBERS OF JUSTICE [REDACTED]

INTERNAL EXCHANGE SERVER PRINTOUT — DOCKET NO. 25-1104
(HOOVER V. UNITED STATES)

CLASSIFICATION: CHAMBERS
CONFIDENTIAL
EXEMPTION: DELIBERATIVE
PRIVILEGE

From: [REDACTED] <[REDACTED]>
To: Justice [REDACTED] <[REDACTED]>
Date: Thursday, October 29, 2026 at 11:48 PM EDT
Subject: **Bench Memo: Hoover v. United States, No. 25-1104 (Oral Argument Prep & Brief Comparison)**

Madam Justice,

Apologies for the late send—I wanted to get the side-by-side chart cleaned up after finishing the reply brief and cross-checking the Joint Appendix before next week's sitting.

I. THE BIG PICTURE: WHAT IS ACTUALLY HAPPENING HERE

On the surface, this is a routine statutory-interpretation appeal about whether a well-meaning network researcher (Mahindra Hoover) gets a jury instruction on the common-law defense of necessity after crashing a huge swath of the domestic internet via Denial-of-Service (DoS) to stop a worse, autonomous zero-day Remote Code Execution (RCE) worm.

Beneath the surface, the Solicitor General is attempting one of the most audacious constitutional judo moves I have ever seen in a criminal brief.

To win his criminal appeal under *United States v. Bailey*, 444 U.S. 394 (1980), Petitioner had to prove two factual premises in the trial record:

1. Autonomous AI exploit swarms move at such blistering machine speed (here, total systemic saturation in 90 seconds) that **human oversight—warrants, phone calls, agency intake queues—is physically impossible.**
2. Once an autonomous swarm starts scanning, the total compromise of every unpatched server on the internet is **mathematically inevitable.**

Look at what the SG just did in the Respondent's Brief: **The Government stipulated to both of Hoover's premises.** Why? Because if the SG can convince five Justices to affirm Hoover's conviction *by holding that 18 U.S.C. § 1030(f) gives the Federal Government an exclusive monopoly over machine-speed digital firebreaks*, Hoover's own factual concessions automatically hand the Executive Branch (and its deputized Tier-1 cloud/ISP contractors)

blanket Fourth and Fifth Amendment immunity to operate a warrantless, uncompensated "kill-switch" over private internet infrastructure in the future.

Put simply: Mahindra Hoover walked into court asking for a jury instruction and accidentally wrote the amicus brief for the NSA.

II. SIDE-BY-SIDE COMPARISON OF THE ARGUMENTS

DOCTRINAL ISSUE	PETITIONER'S ARGUMENT (HOOVER)	RESPONDENT'S ARGUMENT (SG)	WHERE THE ANALYTICAL FAULT LINE LIES
1. Statutory Preemption & 18 U.S.C. § 1030(f) (<i>Oakland Cannabis</i>)	Savings Clause Only: § 1030(f) ("does not prohibit any lawfully authorized... protective... activity" of law enforcement/intel) is a passive jurisdictional carve-out, not a comprehensive regulatory scheme that repeals 400 years of common-law necessity.	Exclusive Sovereign Monopoly: By explicitly naming <i>who</i> is allowed to conduct "protective" cyber-operations (the State), Congress occupied the field (<i>expressio unius</i>). Letting private coders launch counter-worms invites catastrophic false positives and systemic blindness.	The SG has the better policy argument; Hoover has the better text. In <i>Oakland Cannabis</i> , the Controlled Substances Act had an exhaustive scheduling matrix. Section 1030(f) is literally one sentence. Does a single passive sentence "occupy the field" and abolish a common-law trial defense?
2. The Common-Law "Conflagration Rule" (<i>Bowditch v. Boston</i>)	Universal Privilege: At common law, <i>anyone</i> —not just the town fire marshal—had the right to pull down a neighbor's house to stop a spreading fire (<i>Bowditch</i> ; Restatement § 262). Temporary DoS is just pulling down the digital shed.	Epistemic Blindness: A 19th-century bystander could <i>see</i> the shed was empty. A lone coder firing a DoS across routing tables is shooting blind—he can't know if an IP address is a coffee shop or a hospital ventilator network. Only the State has cross-sector visibility.	This is Hoover's weakest point. The SG's distinction between <i>localized physical visibility</i> and <i>blind network interdependency</i> is devastating. If Hoover wins, every cybersecurity vendor with an itchy trigger finger gets to play Fire Marshal in the dark.
3. Fourth & Fifth Amendment Avoidance (<i>Jacobsen / Caltex</i>)	The Avoidance Trap: Do not read § 1030(f) as giving the State a monopoly to crash innocent servers, because if the State did that without a warrant or compensation, it would violate the 4th Amendment (<i>Jacobsen</i>) and 5th Amendment	Calling the Bluff: No constitutional doubt exists! Using Hoover's <i>own</i> machine-speed experts, the SG argues: (1) millisecond propagation = 4th Am. Exigency (no time for a Rule 41 warrant), and (2) mathematical certainty of compromise = 5th Am.	The Danger Zone for the Court. If the Court adopts the SG's Section II to defeat Hoover's Constitutional Avoidance argument, that holding is not dicta —it becomes the binding constitutional predicate for why the government's § 1030(f) power is valid.

	Takings Clause.	"Inevitable Loss" (Caltex/Miller).	
4. Reasonable Legal Alternative (<i>U.S. v. Bailey</i>)	Latency = Futility: Under <i>Bailey</i> , a legal alternative must actually <i>avoid the harm</i> . Calling an FBI 1-800 number when an autonomous worm compromises the grid in 90 seconds is like telling a prisoner in a burning jail to file a grievance (<i>Kirby</i>).	Deputized Machine-Speed Channels: The alternative isn't a phone call—it's feeding the signature into CISA's automated gateway, where deputized Tier-1 ISPs/cloud giants execute immediate, white-listed null-routing under <i>Yearsley</i> derivative sovereign immunity .	The SG is sneaking an elephant into a mousehole. The SG claims Hoover had a "legal alternative" because CISA has pre-deputized private telecoms to pull the plug at machine speed. Did Congress ever actually authorize CISA to deputize private cloud monopolies to crash private servers?

III. SUGGESTED QUESTIONS FOR ORAL ARGUMENT

For Petitioner's Counsel () — Exposing the Anarchy Problem:

- **The "Blind Firebreak" Hypo:** *"In Bowditch v. Boston, when a citizen pulled down a wooden shed to stop a fire, he could look inside the shed first to make sure there wasn't a nursery school inside. When your client fired a recursive DoS payload across 400,000 IPv4 addresses, he couldn't look through the window of a single one of those boxes. If his 'firebreak' had knocked out a regional hospital network and killed forty ICU patients, would he still get a necessity instruction?"*
- **The "500 Vigilantes" Problem:** *"If the attacker moves in milliseconds, no human defender can type fast enough to stop it either—your client had to unleash an automated counter-script. If you win today, tomorrow morning 500 private cybersecurity startups will deploy autonomous, hair-trigger DoS agents. When Vendor A's defensive bot misreads Vendor B's defensive bot and crashes the Eastern Interconnect power grid, is everyone immune so long as their belief was 'reasonable'?"*
- **The Constitutional Avoidance Trap:** *"On pages 9 and 10, you argue the Government couldn't have done what your client did without violating the Fourth and Fifth Amendments. Are you sure you want to press that? If we agree with your experts that these servers were mathematically doomed within 90 seconds, doesn't United States v. Caltex say the Government owes zero Fifth Amendment compensation when it destroys doomed property in an emergency? Aren't you writing the Solicitor General's Takings Clause defense for her?"*

For the Solicitor General () — Exposing the Sovereign Power Grab:

- **The Trojan Horse:** *"General, we granted cert to decide whether one programmer in*

Arlington gets a jury instruction in a five-year CFAA case. In your response brief, you casually ask us to hold that the Executive Branch—and whatever private cloud monopolies it taps on the shoulder—can unilaterally crash hundreds of thousands of innocent American servers without a Rule 41 warrant and without paying a dime of Just Compensation. Can we affirm under Bailey without handing the Government a constitutional blank check for an internet kill-switch?"

- **The Yearsley Statutory Vacuum:** *"Point me to the exact page and line in Title 6 or Title 18 where Congress authorized CISA to deputize Amazon, Microsoft, and AT&T to intentionally inflict Denial-of-Service damage on innocent third-party citizens. Section 1030(f) says 'does not prohibit any **lawfully authorized**... protective activity.' Where is the underlying affirmative grant of authority?"*
- **The 20% False-Positive Taking:** *"Suppose CISA's automated defense bot sees a zero-day swarm and hits the kill-switch, knocking half of U.S. e-commerce offline at a cost of \$10 billion. Afterward, we learn that 20% of those businesses had a custom firewall rule that would have stopped the worm cold. Their servers weren't 'doomed' at all—you just destroyed their uptime to save everybody else. Under your reading of Caltex, do those innocent business owners just eat a \$2 billion loss?"*
- **The T-Minus 10 Seconds Trap:** *"Suppose Mr. Hoover had uploaded the exploit signature to CISA's automated gateway at T-minus 90 seconds, just like you say he should have. And suppose—because CISA's algorithm has never seen this zero-day heuristic before—it kicks the ticket into a human review queue for Monday morning. At T-minus 10 seconds, nothing has happened. Does his common-law necessity defense kick in at T-minus 10 seconds, or does federal law require him to sit on his hands and watch the national power grid burn?"*

Printed copies are in your chair binder for Wednesday's argument.

Respectfully,

██████████

From:	██████████ <██████████>
To:	Justice ██████████ <██████████>
Date:	Sunday, November 8, 2026 at 6:18 PM EST
Subject:	Re: Bench Memo: Hoover v. United States, No. 25-1104 — Post-Argument Strategy (The "Reciprocal Obligation" Path)

Madam Justice,

I spent most of the weekend trying to square Wednesday's oral argument with our options for

Tuesday's Conference, and I think there may be a middle path that boxes in both sides. (Forgive the slightly sprawling structure below; I wanted to get the doctrinal hooks into your inbox before Monday morning.)

Wednesday's argument made clear that we cannot let Hoover win on a broad common-law necessity theory without legalizing 500 private counter-worms. We have to affirm his conviction. At the same time, handing General █████ what she asked for—an unreviewable sovereign monopoly under § 1030(f) to crash private servers at will, shielded from the 4th Amendment by machine-speed exigency, shielded from the 5th Amendment by *Caltex* "inevitable loss," and completely immune when CISA's algorithm sleeps through an attack (her "let the country burn and hope for executive clemency" answer to your final question!)—feels completely untenable.

The Proposal: Welding the Privilege to an Affirmative Obligation

What if we accept the Government's claim to an exclusive monopoly over machine-speed digital firebreaks under § 1030(f), **but hold that the statutory monopoly carries a reciprocal, legally enforceable *obligation* to actually maintain and execute that system?** If the Executive Branch wants to disarm private citizens from pulling down their own digital sheds in a fire, the price of that monopoly is a non-discretionary legal duty to man the firehouse.

There are three doctrinal hooks we could use to build this in the opinion:

1. The Constitutional Hook (*DeShaney* "Restraint on Self-Help" Exception):

Normally under *DeShaney v. Winnebago County*, 489 U.S. 189 (1989), the State owes no affirmative duty to protect property from private attackers. *However*, Chief Justice Rehnquist noted at p. 200 that an affirmative duty *does* arise when the State acts to "restrain[] the individual's freedom to act on his own behalf—through incarceration, institutionalization, **or other similar restraint of personal liberty.**" By using § 1030(a)(5)(A) and § 1030(f) to outlaw common-law self-help on pain of a 10-year felony, the Sovereign has placed domestic network operators in a position of **compulsory defensive dependency**. Having stripped citizens of their baseline common-law right to pull down adjacent nodes in a conflagration, the Fifth Amendment Due Process Clause forbids the State from failing to operate the substitute mechanism.

2. The Criminal Hook ("Conditional Preemption" under *Bailey*):

We affirm Hoover's conviction today because he never even *tried* pinging CISA's automated gateway at T-minus 90 seconds. *However*, we explicitly answer your "T-minus 10 seconds" question in the text of the opinion: we hold that § 1030(f) preempts common-law necessity **only so long as the Sovereign's machine-speed alternative is functionally responsive.** If a citizen submits a verified zero-day signature to the federal gateway and the Sovereign's automated system fails to respond within the

mathematical propagation window, the "reasonable legal alternative" under *Bailey* is exhausted, and the common-law privilege of necessity immediately revives.

3. **The Civil / Administrative Hook (Piercing FTCA & *Yearsley* Immunity):**

To make sure CISA and its deputized Tier-1 cloud providers can't just sit on their hands, we pair the *Yearsley* derivative sovereign immunity analysis with three teeth:

- **Ministerial Mandate under *Berkovitz*:** Once CISA establishes automated machine-speed ingestion under 6 U.S.C. § 659 to preempt private self-help, keeping that pipeline responsive is an *operational/ministerial mandate*, not a policy choice. Under *Berkovitz v. United States*, 486 U.S. 531 (1988), if CISA negligently lets the gateway lag during an autonomous attack, the **FTCA Discretionary Function Exception (28 U.S.C. § 2680(a)) does not apply**—exposing the Government to tort liability for the resulting RCE damage.
- **Strict *Caltex* Boundaries for False Positives:** We hold that *Caltex* Fifth Amendment immunity applies *only* to endpoints that were *in fact* exposed to inevitable compromise. If a deputized ISP uses a sloppy heuristic that knocks *patched or non-vulnerable* servers offline (your 20% hypo), the Government owes **Fifth Amendment Just Compensation** for those non-doomed servers, and a private contractor exceeding CISA's exact parameters loses *Yearsley* immunity under *Campbell-Ewald*.
- **APA § 706(1) Compulsion:** Systemic failure to maintain machine-speed mitigation protocols becomes reviewable as "agency action unlawfully withheld" under 5 U.S.C. § 706(1).

If we write this, Hoover still loses his appeal, CISA gets the headline it wanted, and the Court establishes that the Sovereign cannot claim a monopoly on the fire axe while leaving the firehouse locked. Let me know if you want me to flesh out the *DeShaney* and *Berkovitz* sections tomorrow!

Respectfully,

██████████

From: Justice [REDACTED] <[REDACTED]>
To: [REDACTED] <[REDACTED]>
Date: Monday, November 9, 2026 at 8:32 AM EST
Subject: **Re: Bench Memo: Hoover v. United States, No. 25-1104 — Post-Argument Strategy (The "Reciprocal Obligation" Path)**

Let me make sure I am reading this correctly before we walk into Conference tomorrow morning.

To avoid deciding a four-page criminal appeal on the simple, boring ground that the defendant never even tried to call the cops before blowing up the internet, you want me to ask four of my colleagues to join an opinion that:

1. Overrules *DeShaney sub silentio* for the entire tech sector;
2. Interprets a one-sentence criminal savings clause in Title 18 as an affirmative congressional command requiring the Department of Homeland Security to operate an infallible, sub-second automated national firewall;
3. Waives the sovereign immunity of the United States under the FTCA whenever a government server drops a packet during a zero-day cyberattack, putting the federal fisc on the hook for trillions of dollars in private ransomware losses; and
4. Announces a new constitutional rule that private hackers get a legal green light to launch vigilante Denial-of-Service attacks across the domestic backbone the exact millisecond a CISA API returns a 504 Gateway Timeout.

Did I miss anything, or did you also want us to appoint a Special Master to rewrite the BGP routing tables from the basement of this building?

We are an Article III court, not DARPA. In the real world, when a federal agency fails to do its job, the remedy is a congressional oversight hearing—not a judicial decree turning the United States Treasury into Lloyd's of London and delegating nuclear launch codes to every impatient coder in Arlington whose ticket stays in the CISA queue for nine seconds.

Come down to my office at 4:00, bring a legal pad, and let's figure out how to affirm under *Bailey* on the narrow record before us without losing our minds.

—[REDACTED].

From: [REDACTED] <[REDACTED]>
To: Justice [REDACTED] <[REDACTED]>
Date: Monday, November 9, 2026 at 8:47 PM EST
Subject: **Revised Conference Strategy (Hoover, No. 25-1104) — The "Price of Admission" Framework**

Madam Justice,

Following our late-afternoon whiteboard session in your office, I scrapped the *DeShaney* and *Berkovitz* tort-duty draft entirely. As you pointed out, under *Norton v. Southern Utah Wilderness Alliance*, 542 U.S. 55 (2004), we have zero authority to order DHS how to program its network routers, and we certainly cannot waive the FTCA's discretionary function exception every time an agency algorithm lags.

However, as we walked through on the pad, the "simple" two-page procedural punt under *Bailey*—holding that Hoover loses simply because he didn't ping CISA's automated gateway before launching his DoS script—still has that fatal mathematical hole in the middle of it unless we pair it with a substantive rule on what § 1030(f) requires as a condition of preemption.

Here is the cleaned-up version of the argument we hashed out for Conference tomorrow morning at 10:00, framing **"automated DoS-before-RCE" not as a judicial mandate, but as the statutory predicate—the "price of admission"—for the Government's monopoly:**

I. THE *BAILEY* FUTILITY PROBLEM WE CAN'T FUDGE

When the Chief goes around the table tomorrow, he is going to want a five-page affirmance saying Hoover failed to exhaust his legal alternative under *Bailey*. If we try to leave it there, Justice [REDACTED] or Justice [REDACTED] is going to open the Joint Appendix to pages 142–145:

- **The Undisputed Math:** Both sides' experts stipulated that this autonomous RCE swarm achieved total systemic saturation in **90 seconds**.
- **The Unplugged Fire Alarm:** On cross-examination (J.A. 144), the Government's witness admitted that when CISA's Automated Indicator Sharing (AIS) gateway receives a novel zero-day heuristic it hasn't seen before, its default operational posture is to **flag the anomaly for human analyst review**—a process with a median latency of **42 minutes**.

Under *Bailey*, a defendant's failure to try a legal alternative is only fatal if that alternative

provided a realistic chance "*both to refuse to do the criminal act and also to avoid the threatened harm*" (444 U.S. at 410). We cannot look a dissent in the eye and say Hoover goes to federal prison for failing to pull a fire alarm that the Government admits wasn't wired to a sprinkler system.

II. THE SOLUTION: "FAIL-CLOSED / DOS-BEFORE-RCE" AS THE PREDICATE OF PREEMPTION

As you put it in your office: *You don't get to outlaw the fire extinguisher unless the sprinkler system is actually turned on.*

To simultaneously (1) deny private vigilantes the right to self-help, (2) preserve full sovereign immunity for the Treasury, and (3) stay within Article III boundaries under *SUWA*, we flip General ██████'s oral argument representation into a **conditional rule of statutory preemption**:

1. Holding the SG to Her Word on § 1030(f):

Instead of *ordering* CISA to re-architect its network, we hold that the preemption of common-law necessity under § 1030(f) and *Bailey* is legally conditioned on the Sovereign maintaining the exact "fail-closed" default posture General ██████ claimed at page 17 of her brief. In the era of autonomous, millisecond-scale exploit swarms, a "reasonable legal alternative" under *Bailey* exists **if, and only if, the Sovereign's designated intake architecture is configured to execute an automated, preemptive firebreak (DoS / BGP null-routing) by default** upon mathematical verification of an inevitable RCE threshold, without routing the threat into a human-latency bottleneck.

- **Why Hoover still loses today:** At T-minus 90 seconds, Hoover had no way of knowing whether CISA's gateway would route his specific packet signature to an automated Tier-1 BGP sinkhole or a 42-minute human review queue—he never sent the ping. By failing to trigger the Sovereign's intake switch at all, he forfeited his *Bailey* defense on this record.
- **Why this boxes in the Executive tomorrow:** Our opinion establishes as binding precedent that if CISA chooses, as a matter of discretionary policy, to leave its automated gateway in a "fail-open / wait for human review" posture during a machine-speed attack, **the Government forfeits its *Bailey* and *Oakland Cannabis* preemption in any future prosecution where a researcher does ping the gateway first.**

2. Why This Preserves Sovereign Immunity (*Gaubert & Miller v. Schoene*):

The reason CISA and its Tier-1 cloud deputies currently hesitate to set their defense grid to "automatic fail-closed DoS" is that they are terrified of getting sued for billions when they crash half the economy to stop a worm. Our framework gives them the exact

immunity architecture they need to keep the sprinkler turned on, without exposing the Treasury:

- **FTCA Immunity (*United States v. Gaubert*, 499 U.S. 315 (1991))**: Setting the national cyber-defense posture to **fail-closed** (or fail-open) is a quintessential discretionary policy judgment shielded by 28 U.S.C. § 2680(a). The Treasury faces **zero tort liability** either way; the consequence of choosing "fail-open" is losing criminal preemption under *Bailey*, not paying tort damages under the FTCA.
- **Fifth Amendment Takings (*Caltex & Miller v. Schoene*, 276 U.S. 272 (1928))**: Under *Miller*, the Sovereign may make a categorical policy choice between two incompatible property interests facing contagion (destroying cedar trees to save apple orchards) without paying compensation. Configuring the national defense grid to **preemptive DoS before inevitable RCE** is a valid *Miller / Caltex* sovereign choice: trading temporary downtime of doomed nodes to prevent permanent systemic destruction.
- **Fourth Amendment Exigency (*Michigan v. Tyler*, 436 U.S. 499 (1978))**: Because autonomous agentic propagation renders a human Rule 41(b)(6) warrant temporally impossible, an automated, temporary null-route triggered strictly by verified RCE propagation metrics is a constitutionally reasonable exigency seizure.

III. THREE-SENTENCE PITCH CARD FOR TUESDAY'S CONFERENCE

1. *"I am with the majority to affirm under Bailey because Hoover never even pinged CISA's automated gateway before launching his own worm—he didn't test the legal alternative."*
2. *"However, we cannot write a serious opinion saying a 90-second CISA ping is a viable 'legal alternative' under Bailey while ignoring page 144 of the Joint Appendix, where the Government admits human review takes 42 minutes."*
3. *"To keep five votes together and preempt the dissent, the opinion must hold that § 1030(f) displaces private self-help in machine-speed scenarios **only insofar as** the Sovereign's architecture operates as an automated, fail-closed firebreak—and we should explicitly confirm under Gaubert, Miller v. Schoene, and Caltex that the Government and its Tier-1 deputies have the statutory and constitutional immunity required to make 'automatic DoS-before-RCE' their default posture."*

The one-page case sheet on *SUWA*, *Gaubert*, and *Miller v. Schoene* is clipped to the back of your Conference binder.

Respectfully,

██████████

From: Justice [REDACTED] <[REDACTED]>
To: [REDACTED] <[REDACTED]>
Date: Tuesday, November 10, 2026 at 8:51 AM EST
Subject: **Re: Revised Conference Strategy (Hoover, No. 25-1104) — The "Price of Admission" Framework**

Much better. That threads the needle.

Framing "fail-closed" as the factual predicate for *Bailey* preemption rather than an affirmative mandate keeps us out of the *SUWA* buzzsaw and leaves the Treasury intact under *Gaubert*. More importantly, it calls the Solicitor General's bluff: if the Executive wants an exclusive monopoly over the digital fire axe, they have to actually keep the sprinkler system wired to fire—and we give them just enough *Miller v. Schoene* cover so they have no excuse not to.

Make sure the citation to page 144 of the Joint Appendix (the 42-minute human review testimony) is highlighted on my card. The Chief is going to try to breeze right past the math for a clean five-page affirmance, and I want the exact testimony in hand when I stop him.

Grab your notepad and meet me outside the Conference room at 9:55. Good work pulling this together.

—[REDACTED].