Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.,* 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

DEPARTMENT OF HOMELAND SECURITY *v.* MACLEAN

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

No. 13–894. Argued November 4, 2014—Decided January 21, 2015

In 2002, Congress enacted the Homeland Security Act, 116 Stat. 2135. That Act provides that the Transportation Security Administration (TSA) "shall prescribe regulations prohibiting the disclosure of information . . . if the Under Secretary decides that disclosur[e] would . . . be detrimental to the security of transportation." 49 U. S. C. §114(r)(1)(C). Around the same time, the TSA promulgated regulations prohibiting the unauthorized disclosure of "sensitive security information," 67 Fed. Reg. 8351, which included "[s]pecific details of aviation security measures . . . [such as] information concerning specific numbers of Federal Air Marshals, deployments or missions, and the methods involved in such operations," 49 CFR §1520.7(j).

In July 2003, the TSA briefed all federal air marshals—including Robert J. MacLean—about a potential plot to hijack passenger flights. A few days after the briefing, MacLean received from the TSA a text message cancelling all overnight missions from Las Vegas until early August. MacLean, who was stationed in Las Vegas, believed that cancelling those missions during a hijacking alert was dangerous and illegal. He therefore contacted a reporter and told him about the TSA's decision to cancel the missions. After discovering that MacLean was the source of the disclosure, the TSA fired him for disclosing sensitive security information without authorization.

MacLean challenged his firing before the Merit Systems Protection Board. He argued that his disclosure was whistleblowing activity under 5 U. S. C. §2302(b)(8)(A), which protects employees who disclose information that reveals "any violation of any law, rule, or regulation," or "a substantial and specific danger to public health or safety." The Board held that MacLean did not qualify for protection

Syllabus

under that statute because his disclosure was "specifically prohibited by law," §2302(b)(8)(A)—namely, by 49 U. S. C. §114(r)(1). The Court of Appeals for the Federal Circuit vacated the Board's decision, holding that Section 114(r)(1) was not a prohibition.

Held: MacLean's disclosure was not "specifically prohibited by law." Pp. 5–16.

(a) The Government argues that MacLean's disclosure was "specifically prohibited by law" in two ways: first, by the TSA's regulations on sensitive security information, and second, by Section 114(r)(1) itself, which authorized the TSA to promulgate those regulations. Pp. 5–14.

(i) MacLean's disclosure was not prohibited by the TSA's regulations for purposes of Section 2302(b)(8)(A) because regulations do not qualify as "law" under that statute. Throughout Section 2302, Congress repeatedly used the phrase "law, rule, or regulation." But Congress did not use that phrase in the statutory language at issue here; it used the word "law" standing alone. Congress's choice to say "specifically prohibited by law," instead of "specifically prohibited by law, rule, or regulation" suggests that Congress meant to exclude rules and regulations. In addition, Section 2302(b)(8)(A) creates a second exception for disclosures "required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs." That the second exception is limited to actions by the President himself suggests that the first exception does not include action taken by executive agencies. Finally, interpreting the word "law" to include rules and regulations could defeat the purpose of the whistleblower statute. That interpretation would allow an agency to insulate itself from Section 2302(b)(8)(A) simply by promulgating a regulation that "specifically prohibited" all whistleblowing.

The Government proposes two alternative interpretations, but neither is persuasive. First, the Government argues that the word "law" includes all regulations that have the "force and effect of law." The Government bases this argument on the decision in *Chrysler Corp.* v. *Brown*, 441 U. S. 281, where this Court held that legislative regulations generally fall within the meaning of the word "law" unless there is a "clear showing of contrary legislative intent." *Id.,* at 295–296. But Congress's use of the word "law," in close connection with the phrase "law, rule, or regulation," provides the necessary "clear showing" that "law" does not include regulations in this case. Second, the Government argues that the word "law" includes at least those regulations that were "promulgated pursuant to an express congressional directive." The Government, however, was unable to find a single example of the word "law" being used in that way. Pp. 6–11.

(ii) Likewise, MacLean's disclosure was not prohibited by Section

Syllabus

114(r)(1). That statute does not prohibit anything; instead, it authorizes the TSA to "prescribe regulations." Thus, by its terms, Section 114(r)(1) did not prohibit the disclosure here. The Government responds that Section 114(r)(1) did prohibit MacLean's disclosure by imposing a "legislative mandate" on the TSA to promulgate regulations to that effect. But the statute affords substantial discretion to the TSA in deciding whether to prohibit any particular disclosure. Thus, it is the TSA's regulations—not the statute—that prohibited MacLean's disclosure, and those regulations do not qualify as "law" under Section 2302(b)(8)(A). Pp. 11–14.

(b) The Government argues that providing whistleblower protection to individuals like MacLean would "gravely endanger public safety" by making the confidentiality of sensitive security information depend on the idiosyncratic judgment of each of the TSA's 60,000 employees. Those concerns are legitimate, but they must be addressed by Congress or the President, rather than by this Court. Pp. 14–15.

714 F. 3d. 1301, affirmed.

ROBERTS, C. J., delivered the opinion of the Court, in which SCALIA, THOMAS, GINSBURG, BREYER, ALITO, and KAGAN, JJ., joined. SOTOMAYOR, J., filed a dissenting opinion, in which KENNEDY, J., joined.

SUPREME COURT OF THE UNITED STATES

No. 13–894

DEPARTMENT OF HOMELAND SECURITY, PETITIONER *v.* ROBERT J. MACLEAN

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

[January 21, 2015]

CHIEF JUSTICE ROBERTS delivered the opinion of the Court.

Federal law generally provides whistleblower protections to an employee who discloses information revealing "any violation of any law, rule, or regulation," or "a substantial and specific danger to public health or safety." 5 U. S. C. §2302(b)(8)(A). An exception exists, however, for disclosures that are "specifically prohibited by law." *Ibid.* Here, a federal air marshal publicly disclosed that the Transportation Security Administration (TSA) had decided to cut costs by removing air marshals from certain long-distance flights. The question presented is whether that disclosure was "specifically prohibited by law."

I

A

In 2002, Congress enacted the Homeland Security Act, 116 Stat. 2135. As relevant here, that Act provides that the TSA "shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security . . . if the Under Secretary decides that disclosing the information would . . . be detrimental to the

security of transportation." 49 U. S. C. §114(r)(1)(C).

Around the same time, the TSA promulgated regulations prohibiting the unauthorized disclosure of what it called "sensitive security information." See 67 Fed. Reg. 8351 (2002). The regulations described 18 categories of sensitive security information, including "[s]pecific details of aviation security measures . . . [such as] information concerning specific numbers of Federal Air Marshals, deployments or missions, and the methods involved in such operations." 49 CFR §1520.7(j) (2002). Sensitive security information is not classified, so the TSA can share it with individuals who do not have a security clearance, such as airport employees. Compare Exec. Order 13526, §4.1, 3 CFR 298, 314–315 (2009 Comp.), with 49 CFR §1520.11(c) (2013).

B

Robert J. MacLean became a federal air marshal for the TSA in 2001. In that role, MacLean was assigned to protect passenger flights from potential hijackings. See 49 U. S. C. §44917(a).

On July 26, 2003, the Department of Homeland Security (DHS) issued a confidential advisory about a potential hijacking plot. The advisory said that members of the terrorist group al Qaeda were planning to attack passenger flights, and that they "considered suicide hijackings and bombings as the most promising methods to destroy aircraft in flight, as well as to strike ground targets." App. 16. The advisory identified a number of potential targets, including the United Kingdom, Italy, Australia, and the east coast of the United States. Finally, the advisory warned that at least one of the attacks "could be executed by the end of the summer 2003." *Ibid.*

The TSA soon summoned all air marshals (including MacLean) for face-to-face briefings about the hijacking plot. During MacLean's briefing, a TSA official told him

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.