IN THE SUPREME COURT OF THE UNITED STATES

_____

No. 19A-_____

U.S. OFFICE OF PERSONNEL MANAGEMENT, ET AL., APPLICANTS

v.

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, ET AL.,

_____

APPLICATION FOR AN EXTENSION OF TIME
WITHIN WHICH TO FILE A PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

_____

The Solicitor General, on behalf of the United States Office of Personnel Management and the Director of that Office, respectfully requests an extension of time, to and including February 18, 2020, within which to file a petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the District of Columbia Circuit in this case. The court of appeals entered its judgment on June 21, 2019, and denied the government's petition for rehearing and rehearing en banc on October 21, 2019. Unless extended, the time within which to file a petition for a writ of certiorari will expire on January 17, 2020. The jurisdiction of this Court would be invoked under 28 U.S.C. 1254(1). Copies of the court of appeals' opinion and its order denying rehearing and rehearing en banc are attached.

1. In 2015, the U.S. Office of Personnel Management (OPM) disclosed a series of electronic intrusions into its data systems. App., infra, 4a. Those intrusions permitted hackers to gain access to the personally identifying information of millions of current and prospective federal employees. Ibid.

Numerous suits arising from the instructions were consolidated in the U.S. District Court for the District of Columbia. App., infra, 5a. The claim relevant here is one brought by a union of federal employees and 38 individuals, representing a putative class of more than 21 million individuals allegedly affected by the intrusions. They sued OPM for damages under the Privacy Act, claiming that OPM had "'willfully failed' to establish appropriate safeguards to ensure the security and confidentiality of their private information." Id. at 8a.

The individual plaintiffs claim to face a "risk of future identity theft" as a result of the intrusions. App., infra, 14a. Certain plaintiffs also claim to have suffered some form of fraud or identity theft since the intrusions. Id. at 7a-8a. Those alleged arms vary widely, ranging from "unauthorized charges to existing credit card and bank accounts" to "the filing of fraudulent tax returns in [plaintiffs'] names." Id. at 8a.

2. The district court dismissed plaintiffs' claims for lack of standing. App., infra, 10a. The court found plaintiffs' allegations insufficient "to plausibly support the conclusion" that

they face a "substantial or clearly impending" risk of identity theft caused by the OPM intrusions. Ibid.

A divided panel of court of appeals reversed in relevant part. The majority held that plaintiffs "face a substantial * * * risk of future identity theft," rather than "a merely speculative or theoretical" risk. App., infra, 16a. The majority based that conclusion on the theory that "the OPM hackers * * * have in their possession all the information needed to steal" plaintiffs' identities and that several plaintiffs claim to "have already experienced various types of identity theft." Id. at 15a.

Judge Williams dissented from that holding. App., infra, 53a-69a. He recognized that, in the "typical case[] where hackers break into a commercial entity's servers and steal consumer information * * *, it is generally fair to infer * * * that the hackers plan to, 'sooner or later,' 'make fraudulent charges or assume [the victims'] identities.'" Id. at 55a. But in this case, where "hackers infiltrated a government system and stole sensitive 'government investigation information,'" Judge Williams found it "fair to infer * * * that the hackers 'might well [have been] motivated by a purpose other than identity theft,'" such as espionage. Id. at 55a-56a. (emphasis omitted). Thus, he concluded, it makes little sense that the architects of a "complex, risky, and possibly expensive cybersecurity scheme would have as even one of [their] goals the extraction of small-potatoes sums from

individuals." Id. at 57a. And because "the initial breach occurred nearly two years" before the operative complaint, Judge Williams explained, "one would expect to see * * * a pattern of similar thefts" "if plaintiffs were right about the hackers' motives." App., infra, 59a (emphases omitted). "But there are no such allegations." Ibid. Judge Williams therefore would have held that plaintiffs' risk-of-identity-theft theory "is not plausible in view of" that "obvious alternative explanation of far greater probability." Id. at 58a.

On October 21, 2019, the court of appeals denied panel rehearing and rehearing en banc. App., infra, 70a-71a.

3. The Solicitor General has not yet determined whether to file a petition for a writ of certiorari. Additional time is needed for further consultation with OPM and other components of the Department of Justice concerning the legal and practical significance of the decision and, if a petition is authorized, to prepare and print the petition.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General
Counsel of Record

JANUARY 2020