AN A.S. PRATT PUBLICATION
OCTOBER 2017
VOL. 3 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 8 | OCTOBER 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number .... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [272] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

D.C. Circuit Sets Dangerous Precedent by Immunizing Foreign Governments that Commit Cyber Attacks Against U.S. Companies and Citizens

By Jerry S. Goldman and Bruce Strong*

The U.S. District Court for the District of Columbia issued a decision that substantially curtailed the ability of American companies and citizens to sue public entities, such as foreign governments, that perpetrate harmful cyberattacks here in the United States. This decision was affirmed by the U.S. Court of Appeals for the District of Columbia Circuit. The authors of this article discuss the decision, which immunizes foreign governments from liability under the Foreign Sovereign Immunities Act even when the foreign government specifically directs its cyberattacks against U.S. companies, residents, and citizens, as long as the intent to commit the crime occurred abroad.

After years of coping with escalating risks posed by private cyber criminals, U.S. businesses, citizens, and residents have recently faced mounting risk of cyberattack from government actors. Indeed, the news is full of accounts of state actors including Russia and China allegedly hacking the computer systems of private companies in the United States.

Lawmakers have responded to these threats by enacting laws such as the federal Computer Fraud and Abuse Act and various state laws that punish perpetrators of cyberattacks. Despite these efforts, on May 24, 2016, the U.S. District Court for the District of Columbia issued a decision that substantially curtailed the ability of American companies and citizens to sue public entities, such as foreign governments, that perpetrate harmful cyberattacks here in the United States. On March 14, 2017, the U.S. Court of Appeals for the District of Columbia Circuit affirmed that decision. These decisions immunize foreign governments from liability under the Foreign Sovereign Immunities Act ("FSIA") even when the foreign government specifically directs its cyberattacks against U.S. companies, residents and citizens, as long as the intent to commit the crime occurred abroad.

These decisions hurt American businesses and citizens for the benefit of countries that intentionally target the United States. The law is not as clear as the D.C. courts

* Jerry S. Goldman, a shareholder in the New York and Philadelphia offices of Anderson Kill P.C., and former prosecutor, focuses his practice on complex litigation, general business law, white collar criminal defense, estate planning along with estate and trust administration, employment law, federal and international taxation, and intellectual property. Bruce Strong is an attorney in the firm's New York office, concentrating his practice in insurance recovery exclusively on behalf of policyholders and in corporate and commercial litigation. The authors may be reached at jgoldman@andersonkill.com and bstrong@andersonkill.com, respectively.

described it, and future victims of cyberattacks should not be discouraged from pursuing their claims notwithstanding the D.C. Circuit's ruling.

THE D.C. CIRCUIT CASE

In the case before the D.C. Circuit, *Doe v. Fed. Democratic Republic of Ethiopia*,[1] a U.S. citizen born in Ethiopia and living in the United States sued Ethiopia, alleging that his computer, located in Maryland, became infected with a computer program known as FinSpy. According to the complaint, FinSpy is a system for monitoring and gathering information from electronic devices, including computers and mobile phones, without the knowledge of the device's user. It is allegedly sold exclusively to government agencies and is not available to the general public. Doe attributed the FinSpy infection of his computer to an email sent by Ethiopia, but the email was not sent to him from within the United States.

According to the complaint, the email contained a Trojan horse attachment that tricked Doe into opening it, resulting in the installation of the FinSpy software. FinSpy is able to extract saved passwords from different programs and can record internet telephone calls.

Doe alleged that once FinSpy infected his computer, it began recording the activities undertaken by users of the computer, including Doe and members of his family. Doe also alleged that the FinSpy software installed on his computer communicated with a computer server located in Ethiopia.

The complaint contained two counts: a claim under the Wiretap Act, alleging that Ethiopia illicitly intercepted Doe's data, and a claim under Maryland state tort law for intrusion upon seclusion, alleging that Ethiopia unlawfully monitored and recorded Doe's and his family's private computer activities.

Doe alleged that Ethiopia was not immune from suit for its hack under the noncommercial tort exception in the FSIA. That exception provides that foreign governments are not immune from suit for cases "in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment."[2]

There are two statutory exceptions to the noncommercial tort exception. The first, known as the discretionary function exception, provides that a foreign state's immunity is not waived with respect to "any claims based upon the exercise [of] a discretionary function."[3] The second provides that immunity is not waived for "any

[1] 189 F. Supp. 3d 6, 9-11 (D.D.C. 2016).
[2] 28 U.S.C. § 1605(a)(5).
[3] *See* 28 U.S.C. § 1605(a)(5)(A).

claim arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights."[4]

After analyzing the noncommercial tort exception under the FSIA, the district court dismissed the case against Ethiopia based upon a non-textual, judge-made interpretation of this exception, the so-called "entire tort" rule. Under that rule, even if a foreign state purposefully directs its conduct toward the United States with the intent to harm U.S. citizens, the foreign state is immune from suit unless the "entire tort," not just the injury, occurs in the United States. The district court acknowledged that the "entire tort" rule was at odds with the plain text of the FSIA, that only the "personal injury or death, or damage to or loss of property" has to "occur[] in the United States." In addition, it also is bad policy. A clever foreign country would simply ensure that part of its conduct, designed to injure Americans, occurred outside the United States.

Nevertheless, despite the strong textual and policy arguments against application of the entire tort rule, the district court felt compelled to follow it in light of the legislative history of the FSIA, which suggests that the tort exception was primarily enacted to allow redress for traffic accidents occurring in the United States (even though courts consistently hold that legislative history should not be analyzed if a statute is clear on its face). The D.C. Circuit affirmed on the same grounds — that the entire tort did not occur in the United States.

These two courts glossed over the plain language of the tort exception that supports a broader application. For example, as the district court briefly mentioned, the tort exception is written in a way that only requires the resulting injury, not the conduct to occur in the United States for liability to attach.[5] Further, there are other textual clues that Congress intended the noncommercial tort exception to apply to torts that cause injury in the United States, regardless of where the conduct occurs. For example, the noncommercial tort exception states that it does not apply to "any claim arising out of malicious prosecution [or] abuse of process." If U.S. Congress intended to create the entire tort rule, why would it carve out torts of malicious prosecution and abuse of process? Indeed, it is hard to imagine a situation where a foreign country brings a frivolous criminal case against an individual from entirely within the United States. The entire tort rule is more like a rewriting rather than a reasonable interpretation of the noncommercial tort exception.

The D.C. Circuit decision also attempted to distinguish two cases, *Letelier v. Republic of Chile*,[6] and *Liu v. Republic of China*,[7] where foreign states were subject to suit in the United States even though their "officials or employees" did not act here. The noncommercial tort exception specifically waives the immunity of foreign states

[4] *See id.* § 1605(a)(5)(B).
[5] *See* § 1605(a)(5).
[6] 488 F. Supp. 665 (D.D.C. 1980).
[7] 892 F.2d 1419 (9th Cir. 1989).

for torts committed by "any official or employee." In *Letelier* and *Liu*, the foreign state was not immune even though the tortious acts committed in the United States were allegedly carried out by agents, not an "official or employee" of the state. The D.C. Circuit decision glossed over this important point in distinguishing these cases.

POLICY IMPLICATIONS

Most importantly though, as discussed above, the *Doe* line of cases ignores the huge policy implications that will impact American companies and citizens for years to come. If countries can perpetrate widescale cyberattacks against U.S. companies and citizens without repercussion, all of us are at risk. This will impact how sensitive information is stored, how much insurance will cost to protect against these attacks, and how everyday Americans will protect their personal identifying information, and will raise the cost of doing business of U.S. companies for the benefit of foreign entities. The *Doe* decisions ignore the realities of the digital age, where borders are virtually meaningless, and set up a loophole whereby a foreign state can intentionally harm Americans in the United States so long as part of their intentional conduct occurred abroad. That cannot be the law.