

DIRECTOR

John K. Rabiej

ACADEMIC DIRECTORS

Mitu Gulati

Professor of Law, Duke University

Jack Knight

*Frederic Cleaveland Professor of Law
and Political Science, Duke University*

Margaret H. Lemos

*Robert G. Seaks LLB'34 Professor of Law,
Duke University*

CENTER BOARD

Carolyn B. Kuhl

*Judge, Superior Court of California,
County of Los Angeles*

John W. Lungstrum

Judge, U.S. District Court, District of Kansas

Lee H. Rosenthal

*Chief Judge, U.S. District Court,
Southern District of Texas*

John R. Tunheim

*Chief Judge, U.S. District Court,
District of Minnesota*

David F. Levi

*Dean and Professor of Law,
Duke University*

MANAGING EDITOR

Melinda Myers Vaughn

CENTER COORDINATOR

Ann M. Yandian

Editorial Assistants

Lora Beth Farmer, Janse Haywood,

Dagny Lu, Zachary Newkirk

JUDICATURE

VOLUME 101, NUMBER 4

ISSN 0022-5800

© 2017 Duke University School of Law.

All rights reserved. This publication, or any part thereof,
may not be reproduced without written permission
from Duke University. Views expressed herein do not
necessarily reflect the views of Duke Law School
as an entity or of its faculty.

Requests for reprints may be sent to:

Duke Law Center for Judicial Studies

210 Science Drive | Box 90362

Durham, NC 27708-0362

Phone: 919-613-7073 | Fax: 919-613-7158

Email: judicature@law.duke.edu

Online: judicialstudies.duke.edu

ON JULY 20, 1999, CONGRESS ENACTED THE “Y2K ACT” (Pub. L. No. 106-37) to limit potential litigation caused by computer date-change problems brought on by the year 2000. Many feared the date change could adversely impact virtually all businesses and other users of technology products. U.S. business firms and public agencies began to identify and correct error-prone technologies as early as 1995. Although precise cumulative spending estimates are not available, U.S. businesses and government agencies spent roughly \$100 billion.

On May 25, 2018, a similarly far-reaching — and potentially more disruptive — event is set to take place: The General Data Protection Regulation takes effect and will apply in all European Union member states without the need for states to enact implementing legislation. The GDPR establishes strict requirements for reporting data breaches and adopting procedures to protect individuals' data and privacy.

GDPR contemplates that businesses design their information governance procedures from the ground up to protect personal data by “minimizing the processing of personal data, pseudonymizing personal data as soon as possible, [enhancing] transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, [and] enabling the controller to create and improve security features.” The Act prohibits transfers of data to countries outside the EU that have not enacted the same standards for protection of privacy, including standards governing transfers of information in accordance with litigation discovery demands. The United States has not enacted such standards.

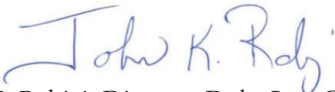
Most U.S. courts have not recognized the force and effect of restrictive foreign data-protection laws when enforcing discovery requests in cross-border disputes. Courts have concluded that comity concerns are not jeopardized when declining to comply with such blocking statutes because the statutes have not provided any substantive right to citizens but were designed mainly to prevent the exercise of U.S. jurisdiction and discovery. Furthermore, there has been little evidence to date that a foreign court would actually impose a severe penalty for violating a blocking statute.

GDPR may change all that. Unlike certain foreign blocking statutes that provided no substantive rights, the GDPR clearly establishes important rights protecting the data and privacy of EU citizens. And, once skeptically regarded as a substantive right here in the U.S., the idea of protecting citizens' privacy has taken on greater respectability and urgency as enormous data breaches become common. But the true game-changer is the penalty for GDPR noncompliance. Companies are subject to a monetary fine of up to \$20 million EUR or four percent of annual revenue, whichever is greater, for each infraction.

In discussions with in-house counsel from multinational corporations, two camps emerge. The first takes GDPR seriously, investing millions of dollars in technology and staff training to become compliant. The second is skeptical, taking a wait-and-see approach, hoping that dire projections, like those projected for Y2K, are not realized.

This high degree of uncertainty extends to cross-border discovery rulings of U.S. courts, which complicate the high-stakes poker U.S. businesses are playing. Courts need to pay attention. After May 25, 2018, transfers of information pursuant to a discovery request that respect GDPR principles — by protecting requested data through protective orders, redactions, and sealing orders and narrowing discovery requests in accordance with legitimate proportionality considerations — may pass muster. Conversely, responses to general discovery requests that ignore GDPR will be subject to potentially harsh sanctions.

The Judicial Studies Center's EDRM, a professional organization that develops e-discovery guidelines and resources, is engaged in an ambitious long-term project to develop GDPR codes of conduct under the leadership of Deena Coffman, BDO Consulting, and Chiara Rustici, independent consultant. One of the main purposes of the codes of conduct is to streamline the procedures for transferring data, including for purposes of discovery. You can read more about the project on Page 8 of this journal and in future editions of *Judicature*, or by visiting EDRM.net.



John K. Rabiej, Director, Duke Law Center for Judicial Studies