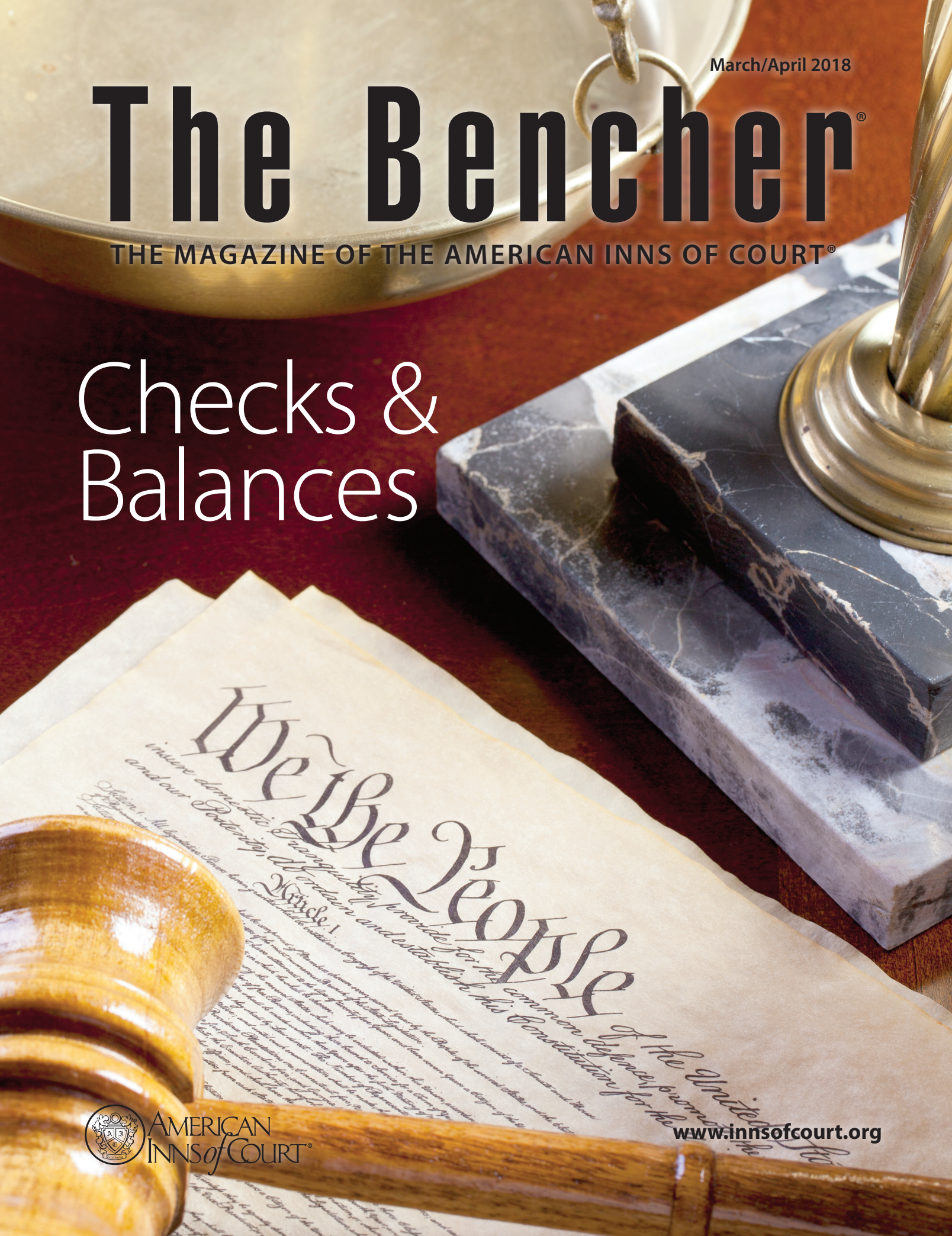
March/April 2018

The Bencher®

THE MAGAZINE OF THE AMERICAN INNS OF COURT®

Checks & Balances



American Inns of Court®

www.innsofcourt.org

TECHNOLOGY IN THE PRACTICE OF LAW

Kevin F. Brady, Esquire

Spotlight on Data Privacy in 2018

Personal data and privacy are under attack. Companies are collecting massive amounts of personal data from customers at the same time cybercrime and data breaches are on the rise. As a result, consumers are becoming concerned about allowing companies to collect their personal information and put that data at risk of being stolen. What can be done? Do consumers have a reasonable expectation that their personal information should be kept private? Are companies meeting the expectations of customers about taking reasonable steps to protect the privacy of customers' data? What is a reasonable expectation of privacy in today's constantly evolving digital world? How does that expectation change based on where the individual is located?

In *United States v. Jones*, 565 U.S. 400 (2012) Justice Samuel A. Alito, Jr., in a concurring opinion discussing the practical limits of the "reasonable expectation of privacy" analysis set out in the 1967 U.S. Supreme Court case, *Katz v. United States*, 389 U.S. 347 (1967), observed that the test in *Katz*:

> rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.

Id. at 427 (Alito, J., concurring) (citations omitted).

FTC Taking Strides to Protect Privacy Regarding Internet of Things (IoT)

On January 16, 2018, the Federal Trade Commission (FTC) announced that it agreed to settle an enforcement action involving internet-connected toys, which it had brought against toymaker VTech for alleged violations of the Children's Online Privacy Protection Act (COPPA). The FTC claimed that VTech, a global supplier of electronic toys for children, violated COPPA by failing to obtain proper parental consent before gathering data from users (parents and children) through its Kid Connect app, and by neglecting to take reasonable steps to secure this data. Vtech's systems were breached in 2015, exposing data collected through the Kid Connect app, which included children's names, ages, photographs, and other personal identifying information. As part of the settlement, VTech is required to pay a $650,000 fine and adopt a comprehensive data security program, and be subject to periodic independent auditing for the next 20 years.

May 25, 2018—Global Data Privacy Day

On May 25, 2018, the General Data Protection Regulation law ("GDPR"), (Regulation (EU) 2016/679),[1] ratified by the European Union (EU) in 2016, takes effect. GDPR is intended to reshape how companies handle data privacy. It was designed to provide EU individuals with greater control over personal information that organizations hold, by strengthening and harmonizing data protection rules for the EU countries. Organizations outside the EU, including the United States, are also subject to GDPR *if and when* they take possession of any data about any EU citizen, wherever that citizen resides.

GDPR defines 'personal data' to include any information relating to an individual ('data subject'), "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Regulation 2016/679 of 4, May 2016, Art. 4, 2016 O.J. (L119), 59 (EU).

GDPR will require transparency into how companies handle personal information. Companies will be required to have privacy policies that are clear, intelligible, and easily-understood. And individual rights have been extended to include the right to know if their data has been stolen, and a "right to be forgotten" if information about an individual is deleted, so third-parties cannot trace them.

The punishment for violation of GDPR can be severe—fines of up to 4% of the company's global revenues or 20 million Euros (approximately $24.5 million U.S.) *whichever is higher*. If that isn't severe enough, GDPR also permits EU member-states the right to impose criminal penalties for non-compliance. ◆

Kevin F. Brady, Esq. is of counsel in the firm of Redgrave LLP in Washington, DC. He is the immediate past president of the Richard K. Herrmann Technology AIC in Wilmington, DE.

1 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679. For additional information about GDPR see, e.g., https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation.