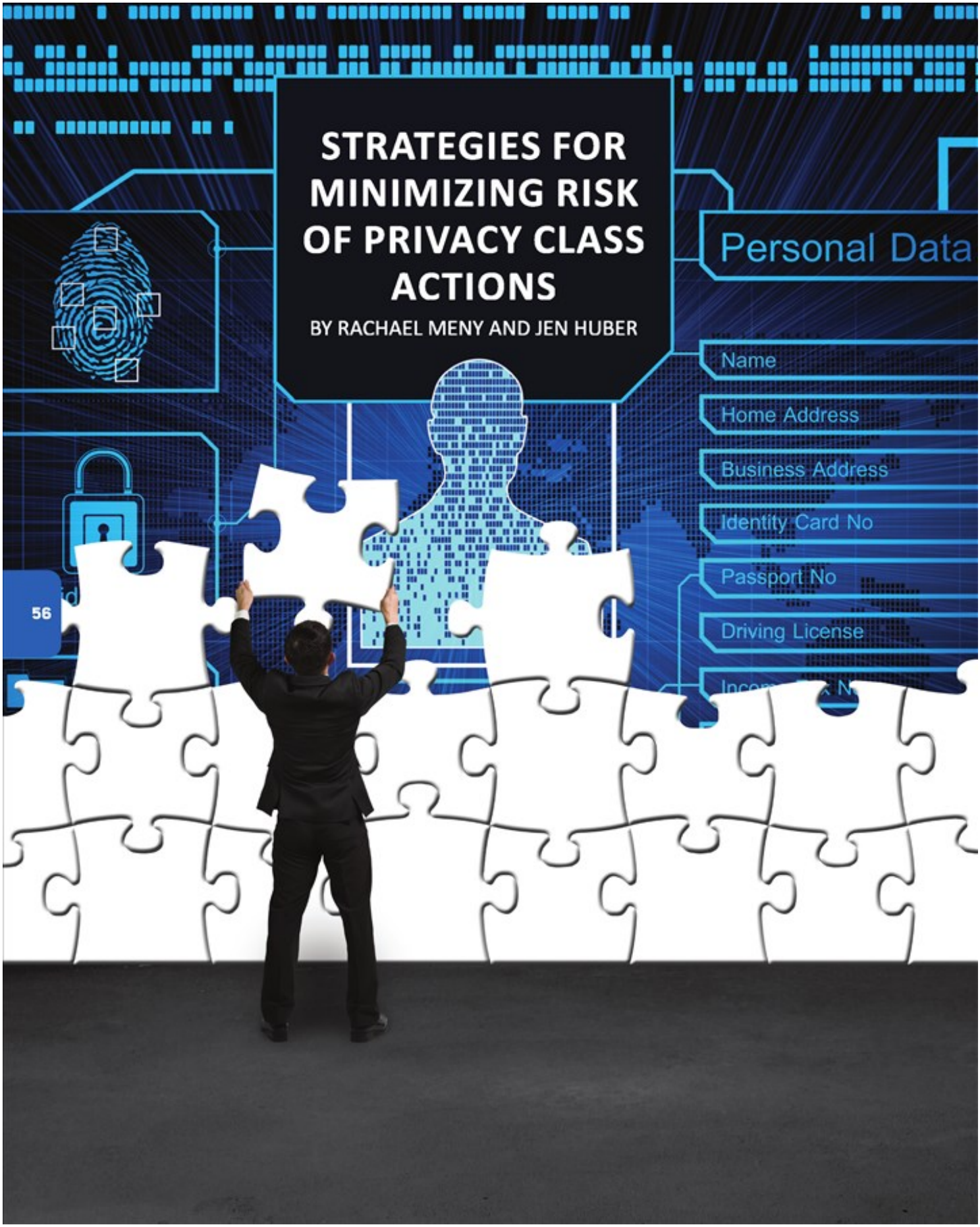
STRATEGIES FOR MINIMIZING RISK OF PRIVACY CLASS ACTIONS
BY RACHAEL MENY AND JEN HUBER
Personal Data
Name
Home Address
Business Address
Identity Card No
Passport No
Driving License
56

Businesses are increasingly facing class action lawsuits alleging they have violated someone's privacy under state or U.S. laws. Most states have privacy statutes, including California with its Invasion of Privacy Act (CIPA), which provides criminal and civil liability for violations like recording communications without consent. Federal privacy statutes include the Electronic Communications Privacy Act (ECPA), which provides criminal and civil liability for intercepting "electronic communications" or permitting access to electronically-stored information. Criminal provisions of these statutes are rarely invoked, but businesses increasingly are seeing civil class action lawsuits under these statutes.

One reason that lawsuits alleging privacy violations are proliferating is that privacy statutes allow plaintiffs to recover both statutory damages and attorneys' fees, such as the $5000 "per violation" award set forth in CIPA. This combination of statutory damages and attorneys' fees encourages plaintiffs' lawyers to file lawsuits based on theoretical privacy injuries, regardless of whether anyone has suffered actual damages.

Defending such claims can be tricky and costly, especially considering that many of these statutes were drafted long ago and do not clearly address modern business practices. Plaintiff lawyers try to exploit these ambiguities, and they are broadening their use of privacy claims to look beyond traditional defendants like telemarketers. A wide range of businesses have been targeted in the past few years, including social-networking companies, Internet companies, App providers and content-streaming companies. These lawsuits have alleged a diverse set of privacy violations for practices such as gathering personal information via a website, App or cookie; using customer data for practices like advertising; and transmitting customer data to third parties, including advertisers.

With these privacy lawsuits proliferating, businesses should take steps now to protect themselves from claims before they are filed, and lay the groundwork for a defense in case they are filed.

PREVENTION STRATEGIES

If your business records, collects or uses consumer data, periodically review your disclosures about these practices to confirm they are accurate and satisfy current law. Good disclosures can include standard and unvarying statements, such as Terms of Service (TOS) and/or Privacy Policies, which describe how information is recorded, used or transmitted. Having good disclosures can help dissuade plaintiff lawyers or help defeat a lawsuit by making clear that consumers know how their information is being used.

Consider whether your TOS or user/customer contracts should include a mandatory arbitration clause or a class action waiver. Businesses that have such clauses should pay attention to the fact that legal requirements vary among states and change over time. Thus user/customer contracts should also be periodically reviewed for legal compliance.

If your business interacts with users/customers, occasionally consult outside counsel about whether your business practices implicate any privacy issues or require privacy-related precautions.

POTENTIAL DEFENSES

Sometimes even the best strategies cannot prevent a lawsuit. If your business is sued for privacy violations, consider the following questions to determine which defenses may apply.

Does the Statute Fit the Alleged Conduct?

Many privacy statutes were enacted before the development of technology like the Internet, and with other kinds of activities in mind. Thus, a viable defense may be that the alleged privacy violation simply does not fit the statute.

For example, the ECPA (enacted during the 1980s to prohibit hacking or eavesdropping) authorizes civil claims for the disclosure of the content of an intercepted communication, but not other communication-related information. Thus, privacy claims involving the interception of information revealing an author's identity or geo-location are not actionable. See *In re IPhone Application Litig.*, from the Northern District of California.

Similarly, sometimes the technology at issue is not addressed by the statute. Claims for unauthorized access under the federal Stored Communications Act, for example, apply only to material in "electronic storage." This law's narrow definition of storage excludes, for example, claims that electronic information like cookies were accessed from a user's computer.

Differing state laws may also enable an argument that one state's laws do not reach those who live outside the state. For example, although CIPA requires all parties to consent to call recording, many other states require just one party's consent. One court dismissed a class action brought by non-California residents under CIPA, finding that the interests of the plaintiff's state of residence would be significantly impaired if California law was applied. See *Jonczyk v. First National Capital Corp.*, from the Central District of California.

Rachael Meny is a partner at the San Francisco law firm Keker & Van Nest. She handles complex civil litigation and white collar cases, including class actions, privacy cases, securities issues, and trade secret and employee mobility disputes. She has litigated cases in state and federal courts throughout California and the United States.
rmeny@kvn.com

Jennifer Huber is a partner at the San Francisco law firm Keker & Van Nest. She handles white collar matters and complex civil litigation, including privacy class actions, securities matters, and trade secret, contract and employee mobility disputes. She has litigated cases before state and federal courts throughout California and the United States.
jhuber@kvn.com

Do Plaintiffs Have an Actual Injury or Standing?
An alleged data privacy violation rarely leads to actual or quantifiable damages, and especially in federal court the absence of injury can be grounds for obtaining dismissal.

To establish standing in federal court, a plaintiff must suffer an "injury in fact" that is "concrete and particularized," and there must be "a causal connection between the injury and the [alleged] conduct." Given these requirements, a number of privacy class actions have been dismissed for lack of standing because the plaintiff suffered no injury in fact. Similarly, a plaintiff may not have standing if a third party (e.g., a hacker) intervened to cause the alleged privacy violation.

Unfortunately, defendants in the Ninth Circuit may be less likely to win dismissal on standing grounds because, in some instances, a statutory violation alone can establish standing. The Ninth Circuit has held that a plaintiff could sue a title insurer under one federal law, regardless of whether she was overcharged, because the statute did not require monetary damages.

But standing is still an important defense to assert and preserve, because the law remains unsettled. Even the Ninth Circuit has never recognized standing on the sole basis of an alleged violation of a state statute, such as CIPA. Moreover, there are differing circuit decisions on this issue, and the Supreme Court has not weighed in.

Did Plaintiffs Consent to the Alleged Practice?
Under many privacy statutes, a consumer's "consent" to a business action is a defense. Thus, even if your disclosure and consent procedures do not dissuade a plaintiff from filing a lawsuit, the fact of "consent" can still be grounds for dismissal. See a California Supreme Court decision, *Kearney v. Salomon Smith Barney, Inc.*

However, the question of what constitutes consent varies from one statute to the next, and sometimes within a given statute. For example, although many states allow calls to be recorded if one party consents, some states require that all parties do so. Similarly, CIPA's numerous provisions require different types of consent, including "consent," "authority or consent" or "express written consent." Thus, your business cannot necessarily assume that obtaining a given type of consent is sufficient to prevent or defend against a privacy class action. Instead, for each business practice that may implicate a privacy issue, you should determine what laws potentially apply and what type of consent is required.

If the applicable TOS and/or Privacy Policies provide clear notice and appropriate consent was obtained, there is precedent in a number of district courts for early dismissal. Keep in mind, however, that some courts, including the Northern District of California, in *Cohen v. Facebook*, have refused to grant early dismissal if there were questions regarding the sufficiency of disclosure or consent.

Lastly, because consent can be a critical defense, businesses should consider maintaining documentation of their TOS or Privacy Policies as they change over time, and/or maintaining records confirming customer consent. These practices may make it easier to obtain early dismissal.

Did Plaintiffs Have a Reasonable Expectation of Privacy?
Privacy statutes often require that plaintiffs have an objectively reasonable expectation of privacy, so it is worth considering whether the communication at issue can support such an expectation. The Ninth Circuit recently upheld dismissal of a CIPA class action in which the plaintiff had called the defendant, his home security provider, to dispute a charge, holding that the nature of this call did not establish an objectively reasonable expectation of confidentiality. Moreover, as discussed below, if individualized allegations are necessary to establish expectations of confidentiality, this can pose a hurdle to class certification.

Are There Fact-Based Defenses to Class Certification?
Under federal law, numerous requirements must be satisfied before a class can be certified, including number of class members, commonality of issues, typicality of the plaintiff claims or defenses, whether there is an ascertainable class, and the predominance of common questions.

Numerous factual issues can create a basis for disputing privacy class action certification. The fact that a company's TOS has changed over time, for example, may defeat commonality. At least some courts have refused to certify a class when potential class members likely received different information, or had different expectations about a business practice, necessitating individual assessment of notice and consent. Similarly, if there is not an easy way to track or identify the instances in which alleged privacy violations have occurred, then certification may be denied because the class is unascertainable. (See *In re Hulu Privacy Litigation* in the Northern District of California.)

Even in the current climate, with the proliferation of privacy class actions, implementing best practices can help your business minimize risk and lay the groundwork for defense. Thinking strategically before a lawsuit is filed and being aware of potential key defenses can often lead to early dismissal. ■