Five Questions General Counsels Should Ask About Cybersecurity and Data Privacy Litigation

Cybersecurity and data privacy litigation continues to grow rapidly in scale and complexity. Putative class actions not only follow major data breaches but also increasingly allege vulnerabilities in a wide range of products, from cars to toys, even before any attack has occurred. And plaintiffs continue to assert privacy claims against both cutting-edge technologies and long-established business practices.

Significant financial and reputational risks can accompany cybersecurity and data privacy litigation. These high stakes make it important for companies to respond strategically and practically. To that end, while each case differs, companies generally should evaluate the following five questions if they face cybersecurity or data privacy litigation.

Does the Plaintiff Have Standing?

Whether a plaintiff has standing to bring suit in federal court continues to be a central question in most, if not all, cybersecurity and data privacy cases. In particular, whether the plaintiff has suffered an injury in fact is frequently pivotal. The US Supreme Court's recent decision in *Spokeo, Inc. v. Robins*, 135 S. Ct. 1540 (2016), clarified that a plaintiff cannot merely allege a technical legal violation but must suffer an actual, real-world injury (or face the certainly impending threat of one). Companies will look to rely on the *Spokeo* decision in the coming years, including as they litigate the types of future injuries that may still be sufficient to confer standing under *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). A judge in the Sixth Circuit recently noted that the US courts of appeals already have split on that latter point, for example, and further significant litigation is highly likely.

Of course, a plaintiff also must adequately allege the other elements of constitutional standing: causation and redressability. A challenged injury may not be fairly traceable to the action of the defendant company but rather be the result of the actions of an independent actor not before the court—like a criminal cyber hacker. Likewise, plaintiffs may seek relief that would not redress the alleged harm, such as a request for injunctive relief to change current cybersecurity practices long after a breach has occurred. (Those allegations also may be subject to challenge for failure to allege a certainly impending injury.) Such infirmities in a plaintiff's standing should not be ignored.

Can the Plaintiff State a Claim?

Courts continue to wrestle with the application of common law and statutory causes of action in the cybersecurity and data privacy contexts. While some claims have

failed consistently across jurisdictions, the availability of other causes of actions has divided courts. Swift dismissal of some or all of these claims may substantially affect a company's litigation exposure. Developing effective challenges to individual causes of action thus remains a key element of any defense against cybersecurity and data privacy litigation. For example, even if a court finds standing, a cause of action may be subject to dismissal because of the failure to allege the type of economic damages necessary to state a cause of action. (Moreover, it bears remembering that a plaintiff or class ultimately will have to prove such damages. Whether a plaintiff or class will be able to prove a significant amount of damages may be a relevant factor to consider in developing the litigation strategy.)

Can a Class Be Certified?

Cybersecurity and data privacy litigation typically involves very limited (if any) injuries to individual plaintiffs. The outcome of a class certification motion consequently can determine whether the litigation can be resolved in a reasonable manner. Plaintiffs' counsel typically try to plead complaints in a manner that minimizes any significant differences in the circumstances and interests of the various members of the putative class. However, an effective motion to dismiss can lead a court to ask a plaintiff to replead a complaint in a manner that brings to light factors that should make it less susceptible to class treatment. And in any event, a company should be prepared to oppose class certification as appropriate, including if numerous individual inquiries would be necessary in light of the unique claims of individual class members. Significantly, this includes being ready to explain why certification of common issues—leaving individualized issues for subsequent resolution—is not appropriate.

How Does Existing Case Law Apply to New Technologies?

Companies facing cybersecurity and data privacy litigation often must apply old doctrines to new technologies. An innovative technology may raise new questions about a consumer's expectation of privacy, for example, or force consideration of how principles developed in data breach litigation should or should not apply to threats involving the Internet of Things. Here, again, companies must think strategically. The decision whether to draw analogies to other technologies—and if so, which technologies—could affect a company long after an individual litigation.

What Are the Collateral Risks of Litigation?

Litigation presents not only direct risks but also collateral risks, whether of regulatory or congressional scrutiny, reputational harm or additional follow-on litigation. A frank assessment of these collateral risks can sometimes argue in favor of prompt settlement (which can be facilitated by a clear presentation of the many legal hurdles facing a plaintiff); in other circumstances, the answer may be to fight back even more vigorously. Whatever the answer, a company will benefit from looking at cybersecurity and data privacy litigation in the context of the broader risk landscape.

* * * * *

The best litigation strategy in any cybersecurity or data privacy case will depend on many factors. Asking the five questions above, however, will help a general counsel build an effective strategy for both resolving the present litigation favorably and mitigating future litigation risks.

For more information about the topics raised in this Q&A piece, please contact any of the following lawyers.

John Nadolenco
+1 213 229 5173
jnadolenco@mayerbrown.com

Robert J. Kriss
+1 312 701 7165
rkriss@mayerbrown.com

Laura R. Hammargren
+1 312 701 8146
lhammargren@mayerbrown.com

Kendall C. Burman
+1 202 263 3210
kburman@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com