Cover Story

A Tangled Web

HOW THE INTERNET OF THINGS AND AI EXPOSE COMPANIES TO INCREASED TORT, PRIVACY, AND CYBERSECURITY LITIGATION

NEARLY EVERY BUSINESS IS GOING THROUGH ITS OWN digital revolution. And every day, more and more companies are realizing that they are a digital company—or need to become one. The digital revolution is transforming not only high-tech companies but also traditional industries whose products, business models, and workforces are being affected by increased connectivity, artificial intelligence, and the ability to collect and use tremendous amounts of data.

Manufacturers use robots and machine vision to make products, and they are building more "intelligence" into those products, from toys to autonomous vehicles. Electric utilities use smart grids to manage the distribution of energy. Agribusinesses use drones and advanced imaging to manage crops. Health care companies use 3D printing to customize medical devices. Chemical producers use collaborative technology, such as blockchain, to track the provenance of products. Banks use AI to improve service and personalize offerings. And the list goes on.

"The increasing sophistication of digitally enabled, intelligent products will drive new litigation in the coming years as these products are inevitably breached, either because a product fails or a cybersecurity incident occurs," says Jeffrey Poston, a Crowell & Moring partner and co-chair of the firm's Privacy & Cybersecurity Group in Washington, D.C. "Newer technologies have been commercialized to the point where people now have smart and internet-connected products in their homes, their cars, and their pockets. These products bring together components and technologies from an ecosystem of companies, and they are very complex and morphing all the time through updates and software improvements. When they fail, litigation will ensue and companies will scramble to reduce and redirect liability."

The rise of AI-enabled products raises new questions—and to date, regulators have not provided much insight into how AI should be used. "The main guidance that's out there is a basic standard that simply says that companies need to make sure that AI works in a way that doesn't create an unreasonable risk of injury," says Cheryl Falvey, a partner at Crowell & Moring in Washington, D.C., and former general counsel of the Consumer Product Safety Commission. "In product liability litigation, however, guidance is one thing and juries are another. In the courtroom, a jury is going to decide whether the things the company did in designing the product were enough to reduce the risk of AI not operating as it should. And when you combine artificial intelligence with the Internet of Things to create what

"The increasing sophistication of digitally enabled, intelligent products will drive new litigation as these products are inevitably breached." **Jeffrey Poston**

the industry calls AIoT, you are pioneering technologies that can impact consumers' lives in a powerful and positive way, but you are also opening up litigation risks that can make or break the long-term viability of a business."

In addition to digitally enabled products breaking, their reliance on vast amounts of data creates ever-evolving risks of breach. "As companies embrace digitalization, they are also facing a new realm of exposure," says Evan Wolff, co-chair of Crowell & Moring's Privacy & Cybersecurity Group in Washington, D.C., and a former data scientist and Department of Homeland Security advisor. That exposure is driven by two phenomena: the increasing sophistication of cyberattacks, and the growing array of statutes and regulations governing data security and, increasingly, data privacy. While the new regulations vary, many create litigation opportunities for regulators, class action plaintiffs, and even whistleblowers—and raise the stakes of that litigation significantly. As a result, says Wolff, "the legal impact of cyber and privacy risk is not just an IT or security issue, and it is not only connected to the possibility of a system breaking. It affects the health and even the survival of the entire business."

Litigating the Internet of Things: When Breaks Harm Consumers

The emergence of smart, connected products has been rapid and widespread. According to the World Economic Forum, there will be more than 20 billion devices connected to the Internet of Things by the end of this year, from smart watches to doorbells, refrigerators, security cameras, and voice-powered assistants. The first wave of product liability attacks against IoT devices foundered on a basic legal problem: the products had not failed. Plaintiffs' lawyers tried to create causes of action based on the potential for failure, but those claims were dismissed for lack of standing.

Now, however, as more IoT devices are in service and performing critical life- and safety-protecting applications, product failures have begun. And as breaks occur, a new wave of tort litigation threatens to derail a company's digital business innovations.

These digitally enabled products, which often involve components from many suppliers and partners, are not only subject to traditional problems such as defective batteries. They can also run into software and connectivity issues that can impair their performance and even lead to safety concerns. These can be difficult to sort out. "With these complex products, we now have enough experience to know that it's never easy to figure out exactly which component or software led to an issue," says Falvey. "We are going to see even more finger-pointing in court about who's liable, as different suppliers dispute whether they are responsible for the product's failure."

Consumer warnings and disclaimers do not necessarily provide protection. The current race to market can drive companies to add functionalities that are sometimes unproven. "There's a general feeling among tech start-ups that you can just disclaim or warn away that lack of performance as a software 'glitch,'" says Falvey. "But when that performance glitch relates to safety, a warning may not be enough. The law is very clear that if you can design away a product defect, you can't just stick a warning on the product and hope things don't go wrong."

The growing role of software also creates some special challenges for litigators. "You might have several software developers contributing to the functionality of the product," says Falvey. To get to the root of the problem, companies may need to carefully scrutinize each piece of software. "But you might not have the right to look into that proprietary software," she says. "So we think there will be litigation fights over discovery asking for software source code as companies try to figure out what went wrong."

One type of software in particular—AI—will play a growing role. With AI, the technology, rather than the consumer, makes various decisions about the product's operation. "If the wrong decision is made and the product does something unsafe, that opens up the manufacturer to responsibility. And it takes away certain defenses that have traditionally been available in a product liability case, such as the consumer's contributory negligence," says Falvey. If an AI-enabled car causes an accident, you can't blame the driver for being contributorily negligent. In future litigation, then, plaintiffs can be expected to push defendants with questions about what the company did to understand its AI capabilities, what inputs were used to guide AI, and how the product was programmed to react to the various inputs it receives.

"AI is dramatically improving business operations, but it is also opening up new frontiers for litigation exposure," says Poston. For example, algorithms used for employment hiring, predicting recidivism, and even bank lending carry risks of bias embedded in AI's machine learning and thus create concerns about discrimination. "As companies improve their products

"Companies need to think about what data they will need to preserve in the event of product liability litigation."
Cheryl Falvey, *former general counsel, CPSC*

Fighting Back

Completely eliminating the risk of a cyberattack is unlikely, but there are things that companies can do to push back, and even go on the offensive. "There are very sophisticated investigative tools that let you collect a great deal of data about the bad actors coming into your network," says Crowell & Moring's Gabriel Ramsey. For example, he says, some companies are employing "denial and deception" techniques that use decoy systems and fake information to make attackers believe that they are successfully working their way through systems to find valuable targets. "You lead them down the path and monitor them and guide them to a quarantined space where they are blocked from the real systems," he says. "Along the way, you can collect a lot of information about how they operate and even who they are."

That knowledge can be used not only to improve cyber defenses but also to pursue the hackers. "Once you identify them, you can use the legal system," says Ramsey. That might mean turning the information over to state or federal investigators, or it might mean a company takes action on its own through lawsuits or cooperation with authorities in other countries to hold the perpetrators accountable. In some cases, companies have an advantage over U.S. officials in such efforts. "They can move more quickly and aggressively, especially when working with partners across borders," he says. "Companies often don't realize they have these options, but these kinds of efforts can be quite effective."

and operations through new technologies, they must carefully assess how those improvements may also expose them to new risks," he says.

The Potential Downsides of Product Data

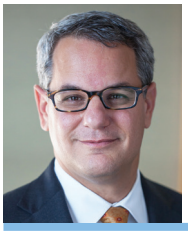
In managing new waves of product-litigation risk, companies will have to pay close attention to the large amounts of data about product performance and usage generated by smart and connected devices. A smart home, for example, might produce 1 gigabyte of data a week, while a connected car might produce 25 gigabytes an hour. Much of the data generated by products can be captured by the manufacturer, but that often doesn't happen. "With today's volumes of data, it can't all be saved—it would cost a fortune. So in many cases, data is constantly being written over or discarded," Falvey says. "Companies need to think about what data they will need to preserve in the event of product liability litigation."

Companies will also need to consider how they use that data. Are they analyzing it proactively to identify performance or safety problems? If not, plaintiffs and regulators may ask why. "Would a reasonable company be using technology to mine that data to help meet a safety goal, for example," says Falvey. "Certainly, companies do that for life-saving products such as pacemakers. To what extent do they need to be thinking of doing it for other types of products where an adverse event might result in a safety hazard?"

With connected, software-enabled products, the data can flow in both directions—and that can help companies stay ahead of liability issues by more easily fixing broken products. For example, companies need to be ready to address hacking vulnerabilities and software problems as they become evident in products. In those cases, says Falvey, "there may be a post-sale duty to inform the customer, if not an express legal obligation to fix it."

Yet repairs can create some gray areas in product liability. "Often, fixing a software glitch in a product can affect the original functionality of that product," Falvey says. "Maybe the battery charge doesn't last as long, or maybe some of the performance characteristics aren't exactly as they were before. When a company decides to fix a product proactively so that something bad doesn't happen, the lawyers need to consider whether any resulting change in functionality may open up the company to consumer protection and deceptive trade practices claims. And what about the fact that the consumer bought the product knowing that it was going to be constantly morphing, like a phone where new apps and functions are always being added? Have they expressly or impliedly consented to product changes over time, or not? These are questions and areas that general counsel should watch."

In the long run, the data generated by connected products could have a far-reaching impact on a range of lawsuits and



"As companies embrace digitalization, they are also facing a new realm of exposure." **Evan Wolff,** *former data scientist and DHS advisor*

trials. "These devices are tracking virtually every aspect of our engagement with the product, not just the product functionality," says Falvey. "They tell us what someone was doing, where they were, how fast they were driving. And that data is going to be incredibly important in litigation."

Data Breaches: The Never-Ending Challenge

As the benefits of technology have spread, so, too, have the challenges associated with data protection and individual privacy. Cyber risk comes in various forms, from individual hackers to company employees downloading sensitive information onto USB drives. Often, however, criminal organizations and state-sponsored actors are involved. "Increasingly, cyber espionage seeks to take advantage of companies' weakest links, including through phishing emails that target companies' intellectual property and other crown jewels," says Paul Rosen, a partner at Crowell & Moring in Los Angeles who is a former chief of staff at the DHS and a former federal prosecutor.

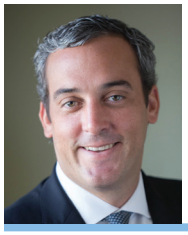
Data breaches involving the loss of hundreds of millions of records have made headlines. But in reality, most breaches are relatively small—the average attack involves just 25,575 records, according to the Ponemon Institute, an independent research group focused on data privacy. "Cybersecurity now impacts virtually every business—from large and midsize companies to small businesses in the United States and around the world," says Rosen. "This phenomenon is likely to continue since businesses are increasingly reliant on and intertwined with the digital economy."

All 50 states now have some sort of data breach notification law in place, and several federal agencies require breach reporting. This has led to a growing number of follow-on class action suits, and defending against those claims has become more complicated. "The go-to defense in these consumer class actions is to argue that the plaintiffs lack Article III standing because the complaint does not assert a concrete and particularized injury and damages are speculative or conjectural," says Poston. "But now we are getting different Circuit Court approaches to the standing analysis." The 6th, 7th, 9th, and D.C. Circuit Courts have ruled that the future risk of identity theft may be enough to provide standing in data breach lawsuits, while the 2nd, 3rd, 4th, and 8th Circuits have said it may not be enough. "These cases are all fact-specific, but these different approaches and outcomes are something to keep an eye on," says Poston. In the meantime, he notes, "the attacks and breaches are not slowing down, and neither are the class action lawsuits."

Government Oversight: A Growing Emphasis on Data Privacy—and Litigation

In early 2019, Congress began to discuss a federal data privacy law. But by midyear, the effort had stalled, largely over the question of whether it would preempt state laws, which could be stricter than the new federal law. "The question of whether a new federal privacy law would preempt state law will be hotly debated because federal presumption would have a direct impact on how states could regulate privacy and cybersecurity that affects their own citizens," says Rosen.

Many states have been filling that gap by passing some form of privacy law, and more are adopting or modifying such laws all the time. On this front, all eyes are on the new California Consumer Privacy Act, which took effect on January 1, 2020. The most extensive of U.S. data privacy laws, it gives consumers control over the collection, use, and sale of their personal data and imposes a number of specific breach-disclosure and operating requirements on companies. Enforcement by the state's attorney general can result in an injunction or penalties of up to $7,500 per intentional violation. It also grants a right of private action, with potential statutory damages ranging from $100 to $750 per California resident and incident (or actual damages, if higher).



"Cyber espionage seeks to take advantage of companies' weakest links, targeting companies' IP and other crown jewels." **Paul Rosen,** *former DHS chief of staff*

"Imagine that a company is sued in a class action by a million people, with damages of $750 per person. That's $750 million in potential liability." **Jennifer Romano**

Companies could find themselves facing a two-pronged challenge, says Jennifer Romano, a partner at Crowell & Moring in Los Angeles and co-chair of the firm's Litigation Group. "Victims of cyberattacks could have to respond to an investigation or inquiry by the attorney general's office while responding simultaneously to a daunting class action complaint filed in the wake of a breach," she says. Importantly, California does not have a constitutional standing requirement to bring suit, and California courts have been less stringent with respect to whether a plaintiff must suffer injury before filing suit. "Having the possibility that any person with data that was involved in a breach can bring a class action creates great potential exposure and risk for companies that are victims of cyberattacks," she says.

Romano believes companies may be able to learn from litigants' past experience with California's Confidentiality of Medical Information Act, which supplements federal HIPAA privacy protections. Both the CMIA and the CCPA provide for statutory damages, which can be sought in class action lawsuits, and neither requires class members to prove they suffered damages or any actual harm. And both "require some sort of unauthorized access, exfiltration, theft, or disclosure of the information," Romano says. "What we've found in cyberattacks is that companies will sometimes know that somebody has gotten into their systems, but they can't tell what data has been viewed or if anything has been accessed." It is then up to the plaintiff to prove a theft took place, and that can be difficult when they can't point to any harm or damage. With CMIA cases, she says, "many courts in California have been careful to hold plaintiffs to their burden to prove that the access or theft actually happened. That case law may be relevant to CCPA cases, and it may not be enough to know that a system has been attacked. Plaintiffs will need to show that their non-encrypted or non-redacted personal information was accessed."

The CCPA could raise other questions as lawsuits work their way through the courts. "There may be some due process arguments being raised," says Romano. "Imagine that a company is sued in a class action by a million people, with statutory damages of $750 per person. That's $750 million in potential liability, even though the company is the victim of an attack and there may be no proof that the class members suffered financial loss."

In the coming years, privacy statutes can be expected to be an ongoing challenge. "Companies are wrestling with how to comply with CCPA and other laws," says Poston. "The bottom line is that you want to be able to demonstrate that you have a serious, thoughtful privacy protection program in place, and you also need to be as practical as possible to create a way for ongoing business operations."

The FTC: The Leading Federal Enforcer on Privacy

Without overarching national laws, the Federal Trade Commission remains the nation's lead data security and privacy enforcer at the federal level—and its view of those issues has significant ramifications for litigation. A few years ago, the FTC seemed poised to take a posture of so-called "regulatory humility," an approach that aims to recognize certain limitations of regulation and avoid overprescription on complex issues. But regulatory humility has not meant inaction. "Over the past year or so, the FTC has been very active and has demonstrated that it intends to exercise its authority as the leading civil enforcer of privacy and data security," says Kristin Madigan, a partner with Crowell & Moring's Privacy & Cybersecurity Group in San Francisco and a former attorney at the FTC's Bureau of Consumer Protection, Division of Privacy and Identity Protection. "The FTC is continuing to pursue major data security matters involving questions of whether companies provided reasonable security for personal information and the representations companies make about their data security."

The FTC has also been actively enforcing the Children's Online Privacy Protection Act. In September 2019, a video-sharing plat-

"The FTC has demonstrated that it intends to exercise its authority as the leading civil enforcer of privacy and data security." **Kristin Madigan,** *former FTC attorney*

Companies should also put themselves in the bad actors' shoes. "Ask yourself, what kind of victim are we? How do the cybercriminals see us?" **Gabriel Ramsey**

form agreed to pay $170 million to settle COPPA allegations that its service had illegally collected personal information from children to support the targeting of ads. Perhaps more important, says Madigan, "the personal information at issue was limited to persistent identifiers—commonly known as cookies—to deliver targeted ads to viewers, and not data such as name, address, email address, or Social Security number that we typically think of as personal information. This settlement pushed the boundaries of what constitutes personal information and a COPPA violation with that definition." The FTC is currently considering updates to COPPA, and those revisions could reflect this broadened view of cookies and other online privacy issues.

On the consumer privacy front, the FTC imposed a $5 billion penalty against a social media giant last year, saying the company had violated a previous FTC order by misleading consumers about its ability to control its own personal information. The penalty was the largest ever imposed for violating consumers' privacy and one of the largest penalties ever assessed by the U.S. government for any violation, according to the FTC.

In such cases, the requirements of the consent orders issued by the FTC are perhaps more important than the amount of a civil penalty, says Madigan, because they provide insights that can help companies avoid litigation. A recent order, for example, required a social media company to restructure its approach to privacy and establish mechanisms to hold company executives accountable for their privacy-related decisions. "The orders in the FTC's landmark settlements provide a baseline understanding of its evolving expectations. These orders can help educate companies about conduct the FTC views as permissible versus not," says Madigan.

In the coming year, the FTC may temper some of its activities. "We expect the FTC will continue to pursue headline-making cases, particularly involving children's privacy and major data or privacy events that affect many consumers," says Madigan. "In areas where there are close calls or truly novel legal questions, the FTC may revert to the more restrained approach that marked the beginning of the current administration." With that in mind, she says, "states and their attorneys general will be another place to watch for cutting-edge privacy and data security issues."

Getting Ahead of the Risks

Companies and legal departments can take a number of actions to adapt to this evolving environment:

Enhance compliance for evolving product liability. With the very real potential for more product liability lawsuits in the digital age, for example, "compliance and litigation-readiness efforts need to modernize to meet the demands of a much more sophisticated product," says Falvey. "The in-house legal team needs to anticipate, from a design perspective, the potential failure modes of products—and then be able to show that the company thought through those issues prior to launching the product."

Toward that end, Falvey says that the legal department needs to be kept in the loop about product design and maintenance decisions, as well as about the plans that the business has for using product-generated data. The legal team can then help ensure that safety and liability issues are understood and, as much as possible, dealt with up front. That's especially important with AI-enabled products. "The functionality of those products is going to evolve after they are out in the marketplace, based on the inputs and 'learning' of the system. A year down the road, the product will not be the same as it was when it was launched. If the lawyers have a seat at the table, they can help you understand future potential liabilities stemming from those evolving products," she says.

Take advantage of technology. On the cybersecurity front, the legal department can work with IT to conduct a risk analysis "and then put together a road map of what technology you need to be using now and in the future in order to better manage your risks," says Gabriel Ramsey, a San Francisco-based partner in Crowell and Moring's Privacy & Cybersecurity Group.

Ramsey also points to data loss prevention, a combination of technology tools and processes that help protect sensitive data. DLP systems identify sensitive and critical data and then monitor the company's end-user computers, corporate networks, and cloud operations to identify any misuse or unauthorized access to that data. "It's tracking things like what's being emailed, what's going out on USB drives, and what's being uploaded to the cloud, and triggering actions in response to suspicious behavior," says Ramsey.

Prepare for cybersecurity events. Companies should develop an incident-response plan that spells out how it will deal with an incident. "It should include a clear governance structure, with clear roles and responsibilities for the response team," says Wolff. A plan should also cover the policies and procedures that will be followed—essentially a playbook for how to respond. "That playbook should then be tested through hypothetical exercises where

GDPR: Recalibrating the Balance of Rights

In a world of increasing privacy regulations, the implementation of the EU's General Data Protection Regulation in May 2018 was a watershed event that recalibrated the balance of rights between citizens, businesses, and governments. The GDPR includes strict rules governing data protection for individuals in the EU—that is, "data subjects"—and gives individuals more control over how their personal data is used. It also allows individuals to sue to enforce the regulation and provides significant penalties. "Under EU law before GDPR, the maximum fine was £500,000. Now it may be up to 4 percent of worldwide annual turnover or £20 million, whichever is higher, which could run into several hundred million dollars," says Laurence Winston, a partner in Crowell & Moring's London office and co-chair of the firm's International Dispute Resolution Group. "So the gravity of the fines is exponentially higher." In the past year, GDPR enforcement actions included, notably, the intention to levy a $230 million fine on a major British company for a 2018 data breach.

"The maximum fine may now be up to 4 percent of worldwide annual turnover, which could run into several hundred million dollars."
Laurence Winston

The GDPR is still relatively new, and some aspects of the regulation are still being worked out. "When data subjects have had their data breached, they are entitled under the GDPR to bring claims for 'material or non-material damage.' The question is, what does non-material damage mean? That's something that's being interpreted by the courts," Winston says. However, he notes, it appears to include loss of control of data regardless of whether plaintiffs suffered actual financial damage or distress that could have huge implications. What's more, even if the individual damages are modest and amount to only a few hundred dollars per claimant, the total damages payable could be enormous in the context of a large class or group action.

In general, Winston says, companies are well aware of the requirements of the GDPR, "but there are still many that are not complying adequately." Often they are struggling with the "unknowns" about the sources and degrees of vulnerability and compliance risk in their systems. "Large companies, especially those that have grown through acquisitions, might have many differently configured systems across many countries," he explains. "Some might be more secure or more compliant than others. A company may even be acquiring systems that have already been compromised and are experiencing a continuing breach. And because companies don't have uniformity of systems, it becomes more difficult to secure data and control the problem."

everyone runs through what they will need to do," he says. "That helps ensure that the organization is ready to respond effectively and efficiently when and if a real incident arises."

Such plans should be overseen and implemented by a cross-functional team that includes representatives from the technology, legal, customer relations, and media relations areas, as well as business units. "A broad team helps bridge the knowledge gap between the technical experts and the senior decision makers and helps employees and executives know what to do," says Rosen. "The team should assess its sensitive data, the technology that's in place to protect that data and prevent attacks, training opportunities for employees, and how to respond if a hack occurs."

Keep learning. Companies should also put themselves in the bad actors' shoes. "Ask yourself, what kind of victim are we? How do the cybercriminals see us?" says Ramsey. "Who would be interested in us? Would they be looking for money, or consumer information, or perhaps IP? That can help you understand the risk you face."

It's also important to learn from the experience of others, as well. "Companies should keep up with other breaches that are publicized—particularly in the same industry—and understand how they occurred and what kinds of technologies were involved to better defend against similar attacks," says Poston.

As the digital revolution spawns new innovation and helps companies create powerful connections with their operations and customers, it can also create a complex web of tort, privacy, and cybersecurity litigation risk. A forward-looking legal and compliance strategy that works hand in hand with the business units of the company can be a critical factor in limiting exposure and driving ahead to a company's digital transformation imperative.