THOMSON REUTERS

Westlaw®

# Internet of things: On the cusp of a litigation explosion

**By Jim Snell, Esq., and Christian Lee, Esq., Perkins Coie LLP***

**NOVEMBER 7, 2017**

In 2015 William Merideth, a 47-year-old father in Kentucky, shot down an $1,800 drone that entered the airspace above his home while his daughters were sunbathing.[1]

Law enforcement arrested Merideth and charged him with first-degree criminal mischief and first-degree wanton endangerment.

According to Merideth, "It was hovering over top of my property, and I shot it out of the sky."

When the drone operators approached Merideth, he brandished his weapon: "I had my Glock on me and they started toward me and I told them, 'If you cross my sidewalk, there's gonna be another shooting.'"

The drone owner contended that he was just trying to take photos of a friend's house.

In the wake of incidents like these, the Federal Aviation Administration and states enacted regulations and laws governing drone registration, limits on their use, reporting requirements and training.[2]

In 2017 an investigator named Troy Hunt reported on security vulnerabilities in internet-connected teddy bears, which recorded children's voices and stored the recordings in the cloud.[3]

The teddy bear company stored the recordings in an allegedly publicly facing network area, which needed no user authentication, and Shodan, a search engine for internet-connected things, indexed the network's location.

Audio files of children's voices and profile photos were supposedly accessible to anybody who had the direct web address. Hunt reported that 2.2 million voice recordings were exposed and apparently obtained by third parties.

These are but two examples of the diverse factual and legal issues associated with connected devices.

We are on the cusp of a swell of civil litigation related to connected devices because, literally, any internet of things device can be "connected."

For this reason, IoT devices can be subject to a wide variety of legal claims.

Nevertheless, there are some common attributes about IoT devices that will likely lead to more litigation.

## MULTITUDE OF WAYS TO RECORD DATA

IoT devices have a variety of sensors, such as microphones, video cameras, location trackers, fingerprint scanners and event recorders, which give them the ability to record different information such as audio, video, geolocation and biometric data.

These characteristics allow for features such as voice-activated commands, such as smartphones and voice assistants; interactivity, including talking toys; location such as software with beacon or GPS technology; monitoring, with security cameras for instance; and biometric recognition, for unlocking devices or identification.

While these features unlock untold innovation and opportunity, they may also give rise to allegations about how companies collect, use and store customers' private information or its information security standards.

Given the variety of technologies that IoT devices may use, the specifics about how the technology works are often very important.

IoT devices may raise different legal issues depending on whether enterprises or consumers use them.

For example, enterprise IoT devices may implicate the security of a company's business data and trade secret information. They also may raise employment law issues.

By contrast, consumer IoT devices face traditional hurdles, such as notice and consent, as well as the collection and use of sensitive data, but in a different context where traditional practices, such as updating software or terms, may be more difficult.

## TERMS OF USE AND PRIVACY POLICIES

Typically, one or more agreements govern IoT devices, such as terms of service or use, as well as privacy policies.

These agreements and policies address, for example, notice and consent to collecting and using data, allocating and mitigating an IoT device provider's risks.

How an IoT device provider delivers terms is critical to their enforceability. If a user alleges ineffective notice or consent, an agreement's enforceability may come into question.

This can mean risk allocation, choice-of-law and arbitration provisions, among other clauses, may be unenforceable as well.

IoT device sellers may find obtaining consent more challenging than traditional internet companies where practices for obtaining consent are more established.

For example, IoT devices such as smart appliances may lack screens, making consent to traditional "clickwrap" agreements — where consumers can click an "I agree" box to show they agree to terms — more difficult to obtain.

It may also be difficult to notify users about changes in policies or terms and obtain any further consent to these terms, if necessary.

IoT devices are hardware products, and products can fail. When they fail, the connected nature of IoT devices can lead to claims.

For example, a hack to a connected pacemaker could lead to tampering to deliberately induce irregular heartbeats, a problem traditional pacemakers do not face.

## DATA SHARING AND INTERCONNECTION

Given that IoT devices can be used to collect, store and share information, personally identifiable information can be widely disseminated among parties and locations, which could include other countries.

As a result, an alleged IoT device failure resulting in a data breach could involve large amounts of data, multiple parties and various geographies.

With respect to alleged vulnerabilities, IoT providers need to be focused on claims by those other than their customers.

For example, in late 2016 it was reported that vulnerable IoT devices were hacked on a large scale to facilitate a botnet denial-of-service attack on popular websites.[4]

These instances can lead to claims from noncustomers.

IoT devices may collect sensitive data, such as information related to children, finances, health conditions and biometric data.

Sensitive information is typically governed by additional specific laws, such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act and the Illinois Biometric Information Privacy Act. These laws can lead to specific claims related to the types of data collected.

## THRESHOLD ISSUE: STANDING

Standing is a threshold issue in federal court litigation.

In IoT cases, as in other cases, standing issues often involve alleged violations of a statute where a concrete injury may not be clear.

In 2016 the U.S. Supreme Court clarified the threshold requirements to establish Article III standing in *Spokeo Inc. v. Robins,* 136 S. Ct. 1540 (2016).[5]

Based on *Spokeo*, claims tied to statutory violations are likely to turn on whether intangible harms constitute concrete injuries to show injury-in-fact, which requires analyzing whether the act complained of violated substantive rights that Congress sought to protect in passing the statute.

In federal court IoT cases, the issue of whether a plaintiff alleging a violation of a statute has given rise to concrete harm is often a threshold issue.

For example, in *Satchell v. Sonic Notify Inc.*, No. 16-cv-4961, 2017 WL 760786 (N.D. Cal. Feb. 13, 2017), the court held alleged Wiretap Act violations were not merely technical without any resulting tangible harm, given the law's history and how it protects a traditional interest: the right to privacy.

## INJURY-IN-FACT: IMMINENCE OF HARM

A related issue related to standing is that of imminence of harm, which involves whether an injury-in-fact is likely to occur.

Issues about actual or imminent harm also have arisen in IoT device cases involving allegations concerning a lack of reasonable security and susceptibility to hacking, for example, in connection with connected cars, video cameras and home monitoring systems.

Following the Supreme Court's most recent guidance on imminence of harm, lower courts hearing IoT cases have dismissed federal claims where they find that the risk of future harm is too speculative.[6]

In one case involving Toyota Motor Corp., for example, plaintiffs alleged that connected cars were susceptible to hacking, but the court dismissed their claims because they did not show that their cars were actually hacked.

The possibility that a potential hacker could attempt to gain control of a vehicle in the future was insufficient, the court said.

However, the court also cautioned that in some instances, a future risk of harm could be sufficient where it was "a credible threat of harm."[7]

At a minimum, plaintiffs in IoT cases must plead credible future injury.

The exact lines of demarcation for standing in federal court will continue to develop in cases following *Spokeo*.

However, it should be noted that Article III standing is a federal, not state, court issue. Thus, if federal court standing does not exist, and a plaintiff refiles in state court, state court standing issues need to be considered.

## ENFORCEABILITY OF TERMS

Traditional notions of contract law remain highly relevant for IoT device companies and possible litigation, especially related to concepts of:

- Notice of and consent to certain practices, such as data collection.
- Acceptance of terms of use that can limit liability, such as arbitration clauses.

As a general matter, terms of use are enforceable if users agree to them.

IoT device companies may use contracts that traditional internet companies have used and that courts have upheld as enforceable: shrinkwrap, browsewrap or clickwrap agreements.[8]

For enforceable shrinkwrap agreements, courts will find use of the product indicates acceptance of the agreement.

Shrinkwrap agreements might be found on a screen display, in instruction manuals, on product packaging or on a website as a browsewrap agreement, where the terms are posted on the website via a hyperlink commonly at the bottom of the screen.

In general, however, courts require proof of assent to the terms in order to find the terms binding.

Courts can also find agreement to terms though a clickwrap agreement, which requires a user to click a box to indicate consent.

For example, an IoT device with a display screen could display the terms and require clicking an "I agree" icon to obtain user consent before allowing the device to be used.

Courts generally evaluate whether the terms of the clickwrap agreement were clearly presented to the consumer, whether the consumer had an opportunity to read the agreement and whether the consumer manifested an unambiguous acceptance of the presented terms.

While the enforceability of terms is highly fact-specific, clickwrap agreements are more often upheld as valid and enforceable compared with browsewrap agreements.

And among clickwrap agreements, those that more prominently confirm assent and provide notice of the terms are more generally likely to be upheld.

With respect to IoT cases, the adequacy of disclosure and assent provided through owners' manuals, product packaging, online privacy notices, and terms and conditions for specific features can be a case-dispositive issue.

Given the often important terms in such agreements, including forum-selection clauses, risk allocation provisions and arbitration provisions, the enforceability of such terms are often a critical threshold issue in IoT litigation.

## LOOKING TO THE FUTURE

Connected devices can readily attract litigation because they have many attributes that allow a variety of legal claims to be asserted against their designers, manufacturers or sellers.

However, these devices may also have attributes that may make it difficult for a litigant to satisfy threshold litigation issues, such as standing or contract-based limitations.

For example, a litigant may have difficulty establishing Article III standing in federal court under *Spokeo* where the harm alleged is merely a technical violation of a statute with an arguably abstract injury.

Similarly, a litigant may not be able to sustain a civil action when he has consented to terms of use that limit his remedies.

If a plaintiff can satisfy threshold criteria such as these, then there are a variety of federal and state law claims that may be asserted in connected device litigation.

## FEDERAL AND STATE WIRETAP LAWS

Attributes of IoT devices make them susceptible to litigation.

IoT device makers or sellers must be aware of numerous potential federal and state law claims that are commonly asserted in litigation involving connected devices, including those based on privacy statutes, business torts and contracts.

IoT devices or apps involving information that can be construed as communications may give rise to claims under the Electronic Communications Privacy Act and similar state laws such as California's Invasion of Privacy Act, both of which prohibit interception of electronic communications.[9]

An example of an IoT case involving the Wiretap Act is *Satchell v. Sonic Notify Inc.*, which concerns a smartphone app that allegedly allowed the phone's microphone to listen for audio beacons to identify the user's physical location for advertising purposes.[10]

In the plaintiff's initial complaint, she alleged the app caused her phone microphone to continually listen and record audio, thereby turning the app and her phone into an illegal bug in violation of the Wiretap Act.

On a motion to dismiss, the court held the plaintiff's allegations that the defendants captured and listened to private conversations without her knowledge or consent were sufficient to establish standing to sue in federal court, but not sufficiently specific to allege an interception under the Wiretap Act.

The plaintiff amended her complaint, and the action is proceeding, but this case illustrates how important it is to understand the specific technology at issue in assessing risk related to potential IoT claims.

## VIDEO PRIVACY PROTECTION ACT

IoT device companies that transmit video content or information relating to a user's video viewing habits may face claims under the Video Privacy Protection Act.[11]

The VPPA creates a private right of action against videotape service providers, including more modern online video

streaming services, that disclose a consumer's personally identifiable information, or PII.

There is a split among the federal appeals courts over whether a subscriber must be a paying customer to be consider a "consumer." Courts also have given differing interpretations to PII under the VPPA.

Given how broadly some courts have construed the VPPA and the capacity of IoT devices to collect, manage and store video viewing information, companies need to be aware of these claims.

## INVASION OF PRIVACY AND INTRUSION UPON SECLUSION

Consumers may say IoT devices collect, transmit or store personal or private information without their consent or beyond the scope of consent, such that a state law invasion-of-privacy claim exists.

In *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015), for example, the plaintiffs claimed connected cars' tracked their driving information, including driving history, vehicle performance and geographic location, and asserted an invasion of privacy claim.

The court granted the defendants' motion to dismiss this claim, however, disagreeing with the plaintiffs' contention that there is a protectable privacy interest in driving habits and geolocation data.[12]

The court also rejected that the plaintiffs had established a credible risk of future harm to have constitutional standing, a prerequisite to suing in federal court.

Drivers were informed about the data collection practices in owners' manuals, online privacy statements, and terms and conditions, the court said, finding this pointed away from a reasonable expectation of privacy in the collected information.

## BIOMETRICS PRIVACY CLAIMS

IoT devices that use measurable human biological or behavioral characteristics to identify an individual, such as fingerprints or facial geometry, may implicate biometric privacy laws.

Potential candidates for biometric claims include:

- Health and fitness wearables that track biometric characteristics.
- IoT devices with security features such as fingerprint readers.
- Smart TVs or other devices with facial recognition software.

The most litigated relevant law is Illinois' Biometric Information Privacy Act, which governs disclosure, consent and retention requirements for entities that collect, store and disseminate biometric data.[13]

BIPA claims have had mixed success, especially if plaintiffs only assert a technical violation of the statute without more.

In *McCollough v. Smarte Carte Inc.* the court held that the plaintiff did not have standing for alleged BIPA violations involving a fingerprint "key" to lock and unlock a rented locker.[14]

The plaintiff claimed the defendant failed to provide notice of the collection of biometric data, failed to publish destruction guidelines and indefinitely retained fingerprint data.

The court dismissed the claims as a technical BIPA violation without a tangible injury-in-fact.

Due to the locker system's nature, the court also noted users would have understood that their fingerprints would have been used and retained regardless of any published policy.

Furthermore, even if the plaintiff did not provide consent for the defendant to retain the data, the court found there was no concrete harm alleged.

In sum, BIPA claims, similar to claims under other statutes, must still satisfy standing requirements by showing more than just technical violations without harm.

With the growing global biometrics market, fueled in large part by the wearables industry and health trackers, companies that make IoT devices that rely on biometric data ranging from facial recognition software to physical health indicators should consider the impact of such laws on products.

## STATE CONSUMER AND UNFAIR-COMPETITION LAWS

Especially in the consumer space, plaintiffs in IoT cases are likely to try to assert state consumer and unfair-competition claims.

State unfair-competition laws provide a cause of action for:

- Unlawful, unfair or fraudulent business acts or practices.
- Unfair, deceptive, false or misleading advertising.

California's unfair-competition law creates an independent cause of action that can be predicated on any other violation of law.

For example, the plaintiffs in the case against Toyota asserted unfair-competition claims based on alleged violations of other laws.

California's Consumers Legal Remedies Act prohibits unfair or deceptive acts and practices taken to deceive a consumer in a transaction. Again, plaintiffs in IoT cases are likely to try to assert CLRA claims as well.

One theory that appears in IoT unfair-competition claims is premised on diminished value where a device allegedly does not have sufficient security and is susceptible to hacking.

The theory is that a user paid a "price premium" for the IoT device that they would not have paid had they known about the vulnerability or practice.[15]

### *Breach of warranty and contract*

Breach-of-warranty claims are often seen in IoT cases involving connected cars because the vehicles are often covered by different express and implied warranties, such as the Magnuson-Moss Warranty Act for consumer products and the Song-Beverly Consumer Warranty Act.

Common law breach-of-warranty claims may be alleged as well.

Breach-of-contract claims based on alleged failure to perform on a promise can also be pleaded in IoT cases.[16]

## OTHER ISSUES

There are a variety of other issues that IoT companies should keep in mind, including:

- Fraud or misrepresentation claims concerning data collection practices, data use, or strength of security or encryption.
- False-advertising claims based on allegedly untrue or misleading statements to induce consumers to buy certain devices.
- Product liability claims arguing the IoT company had the duty to design or manufacture safe products but breached the duty by designing, manufacturing or selling defective products.[17]
- Privacy by design.
- Data security by design.
- Transparent notice of terms.
- Obtain consent to agreements and use of data.
- Listen to feedback.
- Understand your industry.
- Testing.
- Work with experts.
- Reliable partners.
- Make accurate representations.[18]

### *Privacy and data security by design*

The Federal Trade Commission has provided recommendations to IoT providers, including to consider security by design by, among other things:

- Building security into devices.
- Encrypting devices and data according to industry standards.
- Requiring strong passwords.
- Conducting data monitoring and implementing software updates or patches.
- Providing appropriate security training to employees.
- Conducting penetration testing.
- Employing multiple layers of security.
- Implementing reasonable access procedures.

### *Transparent notice of terms and obtaining consent*

IoT providers should also consider transparency in notices and consent requests, including describing what information is collected, how it is used, whether it is anonymized, whether it can be accessed and how long it is retained.

IoT providers should also consider addressing dispute resolution in their terms, including:

- Where disputes may be brought and who can bring them, in arbitration, individual suits or class actions.
- Risk allocation issues, such as who is responsible for obtaining consents from third parties: the provider or user.
- Limitations of liability.
- Choice-of-law provisions.

IoT providers should also consider obtaining clear assent from users to terms and retaining evidence of consent to defend against potential claims.

As just one example, recording of confidential communications under California's Invasion of Privacy Act requires consent of all parties to the communication, and the penalty for failure to do so is $5,000 per incident.

Obtaining and retaining clear consent to record communications, or clearly allocating responsibility for obtaining such consent to the user of an IoT device, is therefore an important consideration.

### *Listen to feedback*

Customers often report security vulnerabilities or other concerns through service calls or written communications.

IoT providers should consider escalation protocols to address and resolve issues before security breaches or lawsuits occur.

### *Understand your industry*

Best practices and standards are in nascent stages in many IoT sectors.

IoT providers should consider participating in industry groups to ensure their understanding while implementing best practices or creating standards.

### *Testing*

IoT providers should consider conducting regular testing of customer experience and IoT device performance, including user sign-up flow or agreement to terms, penetration tests, security vulnerability assessments, and physical site security checks.

Having such policies in place may help identify and address potential legal issues, but the fact that a company is proactive in addressing such issues demonstrates a commitment to provide a privacy-protective and secure device.

### *Work with experts*

Many IoT providers are not experts in privacy, security, or the specifics of the hardware and software technology involved in their products. In this space, however, a strong understanding of the technology, and how privacy and security relate to such technology, is critical. Such providers should consider working with experts to ensure privacy and security by design.

### *Reliable partners*

Many privacy and security issues in the IoT and other spaces stem from failures of partners. IoT companies should consider having strong provisions in place with respect to privacy and security requirements of partners, risk allocation for any failures, audit rights, reporting obligations and other provisions to minimize risk of events and potential litigation.

### *Make accurate representations*

IoT regulatory enforcement proceedings and litigation often involve "unforced errors" where an IoT provider allegedly made a representation about privacy or security, or some other aspect of the device, that is alleged not to be true.

IoT providers should consider processes to ensure technically accurate statements about IoT devices and avoid statements that could become the subject of later litigation.

## NOTES

[1] Father who shot down drone hovering over his house as his daughters sunbathed is arrested and charged - sparking new privacy debate, DAILYMAIL.COM, http://dailym.ai/2iXal2Z.

[2] *See* Unmanned Aircraft Systems, Fed. Aviation Admin., www.faa.gov/uas/.

[3] Troy Hunt, Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages, TROY HUNT BLOG (Feb. 28, 2017), http://bit.ly/2liLzpf.

[4] *See* Jessica Conditt, *Blame the Internet of Things for today's web blackout*, ENGADGET (Oct. 21, 2016), http://engt.co/2A3wKPs.

[5] In *Spokeo*, the Supreme Court held that Article III standing requires the plaintiff to show that he "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, (3) that is likely to be redressed by a favorable judicial decision." An injury-in-fact means "a legally protected interest" that is concrete and particularized as well as actual or imminent, not hypothetical. Importantly, *Spokeo* cautioned that a "concrete" injury not need be "tangible." According to the decision, to determine whether an "intangible harm constitutes injury in fact" for purposes of Article III, "the court must consider both the history and the judgment of Congress" and determine "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."

[6] The Supreme Court most recently issued guidance on imminence of harm in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), which involved a federal law that authorized surveillance against non-U.S. citizens who are reasonably believed to be located abroad. The *Clapper* plaintiffs regularly communicated with individuals who they believed to be surveillance targets, and they claimed injury based on the likelihood that their own communications would be unlawfully intercepted by the federal government. The *Clapper* court found that the plaintiffs failed to establish present injury-in-fact because the "theory of future injury [was] too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'"

[7] *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015). *See also Riva v. PepsiCo Inc.*, 82 F. Supp. 3d 1045 (N.D. Cal. 2015) (because courts will decline invitations to "engage in an ingenious academic exercise in the conceivable to explain how defendants' actions caused [plaintiff's] injury"). While the plaintiffs in *Cahen* claimed that "it's just a question of when" the hacking would occur, the court noted that plaintiffs did not allege that any future risk of harm was "particularized as to themselves" as opposed to a hypothetical risk to car owners in general. Similarly, in *Flynn v. FCA US LLC*, No. 15-cv-855, 2016 WL 5341749 (S.D. Ill. Sept. 23, 2016), a case also dealing with allegations of inadequate security in connected cars, the court held that imminence of harm had not been pleaded. The court noted that, before the risk of future injury turned to actual injury, skilled hackers first would need to hack the cars; the hack would need to occur despite a recall and fix of the cars; the hacker would need to get access to the car's critical systems (not just minor systems such as climate control); and then would need to hijack the systems to cause a wreck. Finding this possibility too remote, the court dismissed the action as too speculative.

[8] *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014); *see also Schnabel v. Trilegiant Corp.*, 697 F.3d 110 (2d Cir. 2012); *Hancock v. AT&T Co.*, 701 F.3d 1248 (10th Cir. 2012); *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17 (2d Cir. 2002); *Berkson v. Gogo LLC*, 97 F. Supp. 3d 359 (E.D.N.Y. 2015) ("For an internet browsewrap contract to be binding, consumers must have reasonable notice of a company's 'terms of use' and exhibit 'unambiguous assent' to those terms."). In general, however, courts require proof of assent to the terms in order to find the terms binding.

[9] 18 U.S.C.A. § 2510; Cal. Penal Code § 630. A violation of the Wiretap Act occurs when a person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C.A. § 2511(1)(a). Wiretap Act violations may also occur when intercepted communications are used under certain circumstances. 18 U.S.C.A. § 2511(1)(b). An electronic communication is "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature." 18 U.S.C.A. § 2510(12). As one federal appeals court summarized, a prima facie Wiretap Act case is established by showing "the defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device." *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3d Cir. 2016). Similarly, a violation of California's law occurs when any person "intentionally taps, or makes any unauthorized connection ... with any telegraph or telephone wire, line, cable, or instrument" or "reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." Cal. Penal Code § 631(a). A California law violation also occurs when any person "intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential

communication. Cal. Penal Code § 632(a). Some courts have construed California's law as coextensive with the Wiretap Act. *See Sunbelt Rentals Inc. v. Victor*, 43 F. Supp. 3d 1026 (N.D. Cal. 2014); *see also NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938 (N.D. Cal. 2014).

[10] 234 F. Supp. 3d 996 (N.D. Cal. 2017). The plaintiffs in *N.P. v. Standard Innovation Corp.*, No. 16-cv-8655, *complaint filed*, 2017 WL 2492257 (N.D. Ill. Feb. 27, 2017), also asserted claims under the Wiretap Act about the defendant's adult stimulation devices and companion apps. The plaintiffs said the app could remotely control the stimulation device in real time, as well as allow users to send messages or video chats. The plaintiffs claimed the app sent private information about the device's use, including the individual's settings, to the defendant manufacturer. The plaintiffs asserted violations of the Wiretap Act based on the alleged communications the app purportedly intercepted. The case settled shortly after filing so there is no decision regarding the theory's viability.

[11] 18 U.S.C.A. § 2710. The VPPA is subject to differing interpretations by the courts, and the 7th U.S. Circuit Court of Appeals has noted the law "is not well drafted" as it is ambiguous and broadly worded. *Sterk v. Redbox Automated Retail LLC*, 672 F.3d 535 (7th Cir. 2012). A federal trial court in California recently determined that VPPA claims have a "deeply rooted" history in the common law right to privacy and thus can satisfy Article III standing in federal courts. *In re Vizio Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204 (C.D. Cal. 2017). Some courts only allow paying customers to bring VPPA claims, rejecting claims from plaintiffs who stream free video content. *See Ellis v. Cartoon Network Inc.*, 803 F.3d 1251 (11th Cir. 2015) ("[A] person who downloads and uses a free mobile application on his smartphone to view freely available content, without more, is not a 'subscriber' ... under the VPPA."), *c.f., Yershov v. Gannett Satellite Info. Network Inc.*, 820 F.3d 482 (1st Cir. 2016) (holding that a user need not make a monetary payment in return for a mobile application to be considered a "subscriber"). Courts also have interpreted personally identifiable information differently under the VPPA. For example, the 1st Circuit has construed PII broadly to include "information reasonably and foreseeably likely to reveal which ... videos [the plaintiff] has obtained." *Id.* at 486. Specifically, *Yershov* held a user's Android phone ID, GPS data and video viewing information qualified as PII under the VPPA. Similarly and directly relevant to IoT devices, the California federal judge in *Vizio* said MAC addresses — which are linked to devices and can be used to obtain highly specific geolocation data — qualified as PII. *Vizio*, 238 F. Supp. 3d at 1223 ("The suffix 'able' means 'capable of,' so 'personally identifiable information' extends beyond a consumer's name."). In contrast, the 3rd Circuit adopted a more restrictive view of what qualifies as PII under the VPPA after analyzing the legislative history. *In re Nickelodeon*, 827 F.3d at 290 (holding that IP addresses are not PII under the VPPA because it is not "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior"). In the 3rd Circuit, it is possible that Social Security numbers, whose commonsense meaning may seem to be "personally identifiable," may not be PII under the VPPA since such information would not permit an ordinary person to identify video watching habits, despite the common belief that such numbers are private. Other district courts have appeared to adopt a higher threshold for what constitutes PII, including a court that held a digital device's encrypted serial number and person's viewing history did not constitute PII. *Robinson v. Disney Online*, 152 F. Supp. 3d 176 (S.D.N.Y. 2015). Another court that held viewing history along with a device serial number did not qualify as PII under the VPPA. *Locklear v. Dow Jones & Co.*, 101 F. Supp. 3d 1312 (N.D. Ga. 2015). The definition of PII under the VPPA can affect whether these claims can survive a motion to dismiss. Under *Yershov*, for example, plaintiffs may argue that the potential to aggregate anonymous pieces of data brings such data within the definition of PII. The 3rd Circuit, however, has cast doubt on this theory, noting "at least with respect to the kind of identifiers at issue here, [this allegation is] simply too hypothetical to support liability" under the VPPA. *In re Nickelodeon*, 827 F.3d at 290.

[12] In *Cahen*, the court contrasted the information at issue there with PII such as names, mailing or email addresses, birthdates, and credit card information that were stolen by hackers in a data breach, which could create a "certainly impending" "credible threat" of future harm. *Id.* at 972 (citing *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014)). By contrast, in *Vizio* the court found that the alleged collection and dissemination of a person's television viewing history, IP addresses, ZIP codes, MAC addresses, product model numbers, hardware and software versions, chipset IDs, region, and language settings did satisfy the pleading standards for invasion-of-privacy claims. 238 F. Supp. 3d at 1223-24. Plaintiffs also claimed invasion of privacy in the adult stimulation device case, *N.P. v. Standard Innovation Corp.*, but the case settled before such claim was tested.

[13] 740 Ill. Comp. Stat. 14/1. Under Illinois' Biometric Information Privacy Act, biometric information is based on biometric identifier such as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The BIPA law includes a number of provisions to regulate the collection, dissemination and storage of biometric identifiers and biometric information. For example, the statute provides that an entity in possession of biometric data must have a written policy made available to the public and have a retention policy to permanently destroy collected biometric data. An entity must also act within a reasonable standard in the entity's industry and have certain notice and consent procedures. The law provides for a private right of action with attorney fees. Other states such as Alaska, Connecticut, Montana, New Hampshire and Washington are considering similar legislation. H.B. 72, 31st Leg., 1st Sess. (Alaska 2017), http://bit.ly/2zf05H1; H.B. 5522, Gen. Assemb., Jan. Sess. (Conn. 2017), 2017 WL 106741, http://bit.ly/2xySNvA; H.B. 518, 65th Leg. (Mont. 2017), http://bit.ly/2ygvsTF; H.B. 523, 2017 Sess. (N.H. 2017), http://bit.ly/2xytdMf; S.H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017), http://bit.ly/2zg0Orh.

[14] No. 16-cv-3777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016). In another case involving scanned faces that were digitized into personalized basketball avatars, the court found that there was no injury where the plaintiff affirmatively chose to scan his face in despite technical failures of notice and consent by the defendant. *Vigil v. Take-Two Interactive Software Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017). Because the plaintiffs could not show their face prints were used or disseminated outside the game, the court found no injury and dismissed the case.

[15] Cal. Bus. & Prof. Code § 17200. *See Cahen v. Toyota Motor Corp.*, No. 15-cv-1104 (N.D. Cal. July 1, 2015), ECF No. 37 at 17-18, based on allegedly concealed defects and violations of other laws, and *Vizio*, 238 F. Supp. 3d 1204, based on alleged violations of other laws. Cal. Civ. Code § 1750. For example, CLRA claims were made in *Cahen* based on allegedly incorrect representations concerning the benefits and safety features of the vehicles, and in *Vizio* based on alleged failures to disclose tracking software on smart TVs. *See Cahen*, 147 F. Supp. 3d at 970 ("Plaintiffs allege that had they known about the lack of electronic security in their vehicles, they would not have purchased their class vehicles or would not have paid as much as they did to purchase them."); *Vizio*, 238 F. Supp. 3d at 1219-20 ("Plaintiffs plausibly allege that they would not have purchased or would have paid less for their Vizio Smart TVs had Vizio properly disclosed its consumer data collection and disclosure practices."); *See generally Kwikset Corp. v. Super. Ct.*, 246 P.3d 877 (Cal. 2011) ("Plaintiffs who can truthfully allege they were deceived by a product's label into spending money to purchase the product, and would not have purchased it otherwise, have 'lost money or property' within the meaning of [the UCL]."). *See also Smith v. Wm. Wrigley Jr. Co.*, 663 F. Supp. 2d 1336 (S.D. Fla. 2009), interpreting the Florida Deceptive and Unfair Trade Practices Act ("Florida courts have allowed diminished value to serve as 'actual damages' recoverable in a FDUTPA claim."); *Ferreira v. Sterling Jewelers Inc.*, 130 F. Supp. 3d 471 (D. Mass. 2015) ("Overpayment can constitute an economic loss that is cognizable under [Massachusetts'] chapter 93A where the consumer continues to own the misrepresented product 'whose value was artificially inflated by a deceptive act or practice at the time of purchase.'").

[16] Under the Magnuson-Moss Warranty Act, 15 U.S.C.A. § 2301, "a consumer who is damaged by the failure of a supplier, warrantor, or service contractor to comply with any obligation under this chapter, or under a written warranty, implied warranty, or service contract, may bring suit for damages and other legal and equitable relief" in federal court. California has a similar law, the Song-Beverly Consumer Warranty Act, Cal. Civ. Code

§§ 1791.1 and 1792. *See Flynn*, 2016 WL 5341749, at 6-7 (alleging breach-of0warranty claims against a connected car manufacturer for cars that were allegedly susceptible to hacking); *Cahen*, No. 15-cv-1104, ECF No. 37 at 24-26 (alleging breach of Song-Beverly Consumer Warranty Act for cars that were allegedly not merchantable and not fit for use in the ordinary purpose); Complaint, *Ross v. St. Jude Med. Inc.*, No. 16-cv-6465, 2016 WL 4527336 (C.D. Cal. Aug. 26, 2016) (pleading breach of express warranty for representations made about benefits of remote-controlled pacemaker that was susceptible to hacking). In *Flynn*, the manufacturer defendants had allegedly limited the plaintiffs' remedies to repairs and adjustments needed to correct defects, rather than allowing for other remedies. Amended Class Action Complaint, *Flynn*, No. 15-cv-855, 2015 WL 11018515 (S.D. Ill. Dec. 22, 2015). Plaintiffs construed the repairs and adjustment remedies as warranties under California state law, but also pleaded in the alternative that when defendants failed to repair their cars, they breached repair contracts with plaintiffs.

[17] *See Ross v. St. Jude Med.*, 2016 WL 4527336. The plaintiff alleged negligence for breach of duty to exercise reasonable care in safeguarding and protecting pacemakers from unauthorized access and use.

[18] *See* Fed. Trade Comm'n, Internet of Things, Privacy & Security in a Connected World (2015), http://bit.ly/1MUraxL.

*This article first appeared in the November 7, 2017, edition of* Westlaw Journal Intellectual Property.



## ABOUT THE AUTHORS

**Jim Snell** (L) is a partner in the privacy and data security group at **Perkins Coie LLP** in Palo Alto, California. He represents and counsels clients on a wide range of complex commercial matters, including privacy and security, internet marketing, and intellectual property litigation and matters. He can be reached at jcnell@perkinscoie.com. **Christian Lee** (R) is an associate in the firm's privacy and data security group in Palo Alto. He focuses his practice on privacy and data security matters and patent litigation. He can be reached at clee@perkinscoie.com.