Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | September 2017

This month we cover a variety of important recent developments impacting the growing insurance-related disputes involving privacy and security coverage, how drones are changing disaster recovery efforts, and the security requirements of Internet of Things (IoT) devices.

Ted Brown and Kat Scott examine the implications of a recent decision by the U.S. Court of Appeals for the Ninth Circuit regarding insurance policies, invasion of privacy, and the Telephone Consumer Protection Act (TCPA). Next, John Lin examines the rise in use, and recognition, of drones as significant disaster-relief tools. Also on the insurance front, Marc Rindner, Ted Brown, and Bonnie Wise address ramifications a double-data breach could have on an organization's cyber insurance coverage policy. Lastly, Megan Brown, Matt Gardner, and Moshe Broder analyze the recently introduced IoT Cybersecurity Improvement Act of 2017.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

ALSO IN THIS ISSUE

No Insurance Coverage for TCPA Claim Under Private Company D&O Policy

By Edward R. Brown and Kathleen E. Scott

The U.S. Court of Appeals for the Ninth Circuit, applying California law, has held that an invasion of privacy exclusion in a directors and officers (D&O) policy barred coverage for a claim alleging violations of the Telephone Consumer Protection Act (TCPA), which, among other things, creates consent requirements for automated calls and text messages to consumers. *Los Angeles Lakers, Inc.*

continued on page 2

Drones to the Rescue After Harvey

By John T. Lin

A new tool is emerging to assist in disaster-relief efforts: drones. Drones are playing a big role as Houston and south Texas recover from Hurricane Harvey. Although the Federal Aviation Administration (FAA) imposed a Temporary Flight Restriction limiting aircraft in the disaster region, it **issued** more than a hundred unmanned aircraft system (UAS) authorizations to operators aiding the recovery. These authorizations are for operations using drones to help locate and rescue victims; survey the damage caused by the flooding; inspect critical infrastructure like railroads, bridges, power lines, and cell towers; ensure communications among first responders; and help insurance companies assess damage to homes and businesses to speed up the claims process. The FAA also issued authorizations to media covering the hurricane, who provided the world with **incredible images of the damage**.

People have used drones in disaster-relief efforts before. Last year, a **civilian drone operator** led to the discovery and rescue of a North Carolina resident who was trapped in his flooded home during Hurricane Matthew. But the use of drones is more widespread and recognized in this effort, marking an important milestone for drones that will almost certainly lead to their increased use in future disaster-relief efforts. Interestingly, some of the authorized operations in Texas – such as flying beyond the operator's visual line-of-sight – are prohibited under current rules, foreshadowing possible rule changes that will make drones more effective in these (and other) situations.

As drones become an increasingly popular disaster-relief tool, new and innovative uses – from delivering food and supplies to conducting broader search-and-rescue missions – will come as well. These uses will help speed recovery times for areas hit by natural disasters. ■

For more information, please contact:

John T. Lin
202.719.3570
jlin@wileyrein.com

No Insurance Coverage for TCPA Claim Under Private Company D&O Policy

continued from page 1

v. Federal Ins. Co., No. 15-55777, 2017 WL 3613340 (9th Cir. Aug. 23, 2017).

The Underlying TCPA Case

The insured, a professional basketball team, was sued for violations of the TCPA after it sent text messages to numerous individuals. Specifically, the basketball team invited fans in the arena to text a message to a short code for the message to appear on the arena's screen. When fans texted the short code, they received the following response text:

> Thnx! Txt as many times as u like. Not all msgs go on screen. Txt ALERTS for Lakers News alerts. Msg & Data Rates May Apply. Txt STOP to quit. Txt INFO for info

In the underlying TCPA case, *Emanuel v. Los Angeles Lakers, Inc.*, No. CV 12-9936-GW, 2013 WL 1719035 (C.D. Cal. Apr. 18, 2013), the plaintiff, who received this response text after texting the team's short code, alleged that the basketball team had violated the TCPA because the response text was an

continued on page 4

'Relatedness' Issues Under Cyber Insurance Policies

By Marc E. Rindner, Edward R. Brown, and Bonnie T. Wise

When responding to a data breach, companies typically undertake a comprehensive forensic investigation to evaluate the potential extent of the incident, the vulnerabilities that enabled the compromise, and the appropriate remediation measures. It is not uncommon for an organization in the process of such an investigation to find indicia that a different compromise may have occurred as well. Identifying the existence of a second breach may considerably alter the scope of the organization's response to the first event and may impact any third-party claims in a significant way.

The discovery of a second breach can have meaningful implications for the organization's cyber insurance coverage. After first analyzing threshold trigger issues under the operative insuring agreements, the starting place for analyzing these issues is under "related claims" policy language, which in effect operates to render two (or more) distinct events or claims to be deemed a single event or claim for purposes of insurance coverage. Different policy forms accomplish this same general objective in different ways. At the most fundamental level, deeming the claims "related" will dictate whether and to what extent the relevant cyber policy will respond. The implications of this analysis include whether: (1) the insured need only satisfy one retention before coverage is triggered; (2) only one limit of liability applies; and (3) events discovered after an operative policy period are deemed to have been discovered previously during an earlier policy period. Relatedness may also bear on other policy provisions that are often implicated by claims under cyber policies.

While case law specific to cyber policies is still in the early stages of development, there is a large body of authority analyzing relatedness under other types of insurance policies. This authority confirms that when the relevant policy terms (such as "related" or "interrelated") are defined, courts focus on that language rather than looking to common law definitions as developed through case law. *See Nomura Holding Am., Inc. v. Fed. Ins. Co.*, 629 Fed. App'x 38, 40 (2d Cir. 2015) (affirming district court's conclusion that claims were related but observing that it erred in employing a "factual nexus" test, noting instead that the district court should have simply applied the plain language of the policy). When left undefined, terms such as "related" or "interrelated" are commonly understood and used to broadly encompass both logical and causal connections. *See*, e.g., *Bay Cities Paving & Grading, Inc. v. Lawyers' Mut. Ins. Co.*, 855 P.2d 1263, 1271, 1274 (Cal. 1993). "Relatedness" may not encompass every conceivable logical relationship, however, such as where the link between the claims or events is extremely attenuated. *See* id. at 1275.

When addressing third-party claims resulting from a series of data breaches, the related claims analysis may be guided by the fact that the claims are premised on a single element of harm or by a single cause. Many courts find these factors significant in assessing relatedness. *See*, e.g., *Kilcher v. Cont'l Cas. Co.*, 747 F.3d 983 (8th Cir. 2014) (wrongful acts asserted against a financial adviser by different claimants in a series of different claims were logically connected because the insured engaged in the same method or modus operandi, notwithstanding that each claimant met with the insured separately; invested different amounts in

continued on page 6

continued from page 2

unsolicited automated text. The district court dismissed the plaintiff's claim, explaining that he voluntarily texted the team, and that the "single confirmatory response challenged here is simply not actionable under the TCPA." Nevertheless, the plaintiff appealed to the Ninth Circuit, an appeal that was eventually dismissed following the team's settlement with the plaintiff. *Emanuel v. Los Angeles Lakers, Inc.*, No. 13-55678 (9th Cir. Apr. 29, 2014).

The Coverage Litigation

The basketball team tendered the suit under its D&O policy. The insurer denied coverage on the basis that the policy barred coverage for any claim "based upon, arising from, or in consequence of … invasion of privacy …." After disputing the denial, the basketball team filed a coverage action against the insurer, arguing that the underlying suit alleged only economic injuries and did not seek damages for the violation of privacy interests. The district court granted the insurer's motion to dismiss and held that the invasion of privacy exclusion barred coverage for the underlying suit. The team appealed.

On appeal, the Ninth Circuit affirmed the dismissal in favor of the insurer. First, after citing the language of the exclusion, the court concluded that the breadth of the exclusion (in light of the "arising from" and "based upon" lead-in language) required only "a minimal causal connection or incidental relationship" between the underlying claim and any invasion of privacy. Next, the court analyzed the phrase "invasion of privacy" and the TCPA, ultimately concluding that "a TCPA claim is, by its nature, an invasion of privacy claim." On that basis, the court held that the complaint, which only alleged violations of the TCPA (and specifically disavowed personal injury claims), was barred by the invasion of privacy exclusion. It affirmed the dismissal in favor of the insurer on that basis.

In a concurring opinion, one judge concluded that while the underlying claim alleged violations of privacy, the court need not determine that all TCPA claims are necessarily claims for invasion of privacy. In a dissenting opinion, another judge suggested that because a TCPA plaintiff is not required to prove invasion of privacy, and because the plaintiff in the underlying case expressly disavowed common law invasion of privacy claims, the invasion of privacy exclusion did not apply.

Important Implications

The Ninth Circuit's decision is important for a number of reasons. First, it is the third case finding no coverage for TCPA claims under Private Company D&O policies. *See LAC Basketball Club Inc. v. Fed. Ins. Co.*, No. CV 14-00113 GAF FFMX, 2014 WL 1623704 (C.D. Cal. Feb. 14, 2014); *Resource Bank v. Progressive Cas. Ins. Co.*, 503 F. Supp. 2d 789, 797 (E.D. Va. 2007). The decision was also the first ruling on this issue from a federal appellate court.

Many other types of insurance policies contain exclusions, like those for invasion of privacy or otherwise, that also bar coverage for TCPA claims. Therefore, organizations facing exposure from claims for violations of the TCPA may be likely to find that their insurance policies do not respond.

The absence of insurance coverage may have a major financial impact on companies facing TCPA exposure. **First**, the cost of TCPA non-compliance is steep. The TCPA imposes statutory damages of $500 per violation, an amount that can be trebled to $1500 per violation if the caller is knowing

continued on page 5

or willful. These statutory damages can add up to astronomical amounts quickly. As examples, in 2016, a cruise line agreed to pay up to **$76 million** for alleged automated calls in violation of the TCPA, and in 2015, a court approved a **$75 million** class settlement involving a large bank.

Second, the volume of TCPA suits has exploded over the past several years. In 2007, there were 14 TCPA claims filed by unique consumer plaintiffs; in 2016, there were 4,860. *See* **2016 Year in Review: FDCPA Down, FCRA & TCPA Up,** *Webrecon* (Jan. 24, 2017). In the 17 months since the Federal Communications Commission (FCC) issued an Order in July 2015 (discussed **here**), a total of 3,121 TCPA lawsuits have been filed in federal courts – which was a 46% increase in the number of suits from the 17-month period immediately before. In addition, many TCPA lawsuits (including more than 1,000 after the July 2015 FCC Order) are putative class actions – driving up the costs of defending and resolving claims.

Third, TCPA compliance is complex. The environment for companies reaching out to consumers via automated calls and texts is fraught with uncertainty and risk, due in large part to the FCC's July 2015 Order, which significantly broadened the scope of the TCPA. The July 2015 Order is currently being challenged in the U.S. Court of Appeals for the D.C. Circuit. The D.C. Circuit may provide a much-needed check on the FCC's broad interpretation of the statute; however, that is yet to be determined. Another factor that contributes to the complexity of TCPA compliance is that much interpretation of the TCPA occurs in various district courts, resulting in oftentimes conflicting takes on the statute.

Given the potential for significant and uninsured exposure, and the complexity associated with compliance, companies should invest in legal compliance on the front end to minimize risk and develop practices do not run afoul of the TCPA.

For additional information, please contact:

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

Draft IoT Legislation Increases Obligations on Contractors and Promotes Vulnerability Disclosure

By Megan L. Brown, Matthew J. Gardner, and Moshe B. Broder

The Internet of Things (IoT) Cybersecurity Improvement Act of 2017, introduced August 1, 2017, by U.S. Senators Mark Warner (D-VA), Cory Gardner (R-CO), Ron Wyden (D-OR), and Steve Daines (R-MT), seeks to improve the security of IoT devices by establishing requirements for IoT devices procured by the federal government. Several third-parties contributed to it, including think tanks and security vendors. It does not appear that the private-sector suppliers of IoT devices or network operators were involved in the drafting.

If enacted, the law would have significant impacts. Among other things, it would require

continued on page 7

different life insurance products; invested at different times over many years; and suffered losses in different amounts); *WFS Financial, Inc. v. Progressive Cas. Ins. Co.*, Inc., 232 Fed. App'x 624, 625 (9th Cir. 2007) (suits "filed by two different sets of plaintiffs in two different fora under two different legal theories" involved interrelated wrongful acts because they were both premised on the insured's alleged "business practice" with respect to the mark-up of the insured's loans); *Brecek & Young Advisors, Inc. v. Lloyds of London Syndicate 2003*, 715 F.3d 1231, 1239 (10th Cir. 2013) (applying New York law) (concluding that claims arising from a common scheme were "interrelated"); but *see*, e.g., *Am. Guar. & Liab. Ins. Co. v. Chicago Ins. Co.*, 105 A.D.3d 655, 656-57 (N.Y. App. Div. 2013) (holding that claims from senior citizens who all responded to the attorney's mass market mail campaign and later lost money when the attorney referred them to a financial services representative who in turn stole their money were not the "same or related" because the attorney "provided separate services to multiple clients"); *Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Ambassador Grp., Inc.*, 691 F. Supp. 618, 623-24 (E.D.N.Y. 1988) (interpreting "interrelated acts" language as not applying to common "mismanagement" of company, instead highlighting that the claims involved "legally distinct claims that allege different wrongs to different people").

Relatedness in the context of first-party cyber coverage involves a similar (albeit distinct) analytical framework. The key difference is that the inquiry does not look to the allegations of the claims – because there is no "claim" asserted by a third party – but instead focuses on the facts uncovered in the investigation. Certain facts that may be particularly important in assessing relatedness include commonalities in the vulnerabilities exploited, the attack vectors, information compromised, identity of the wrongdoers, and other similarities.

Insurers need to recognize the unique coverage considerations when assessing "related claims" issues under cyber policies. Unlike third-party claims, where the insurer and insured may very well be on a "level playing field" in assessing relatedness, relatedness in the first-party context is different because the insured is, at least in the first instance, in control of the relevant information (in many jurisdictions, relatedness for third-party claims may focus solely on the language of the relevant policy and the language in the relevant pleadings. By contrast, some other jurisdictions may permit the introduction of extrinsic evidence to analyze relatedness.) Therefore, the insured may attempt to decide what to disclose (or not to disclose) to its insurer. While an insurer can protect itself to a certain extent by incorporating cooperation requirements in its policies (and by including detailed requirements with respect to proofs of loss), an insured may elect to fight disclosing certain information to its insurer, or otherwise attempt to obscure relevant facts, if it believes doing so would help it avoid an unwanted coverage outcome. Insurers should vigorously avail themselves of the rights set forth in the policy terms the parties bargained for at the outset of the contracting relationship.

Given the potential asymmetry of information, insurers should carefully review and analyze information provided and follow up frequently in order to ensure that their rights are being adequately protected. Insurers at a minimum must ask the "right" questions – and make

continued on page 7

'Relatedness' Issues Under Cyber Insurance Policies *continued from page 6*

sure they get clear answers – when related claims issues may be presented. Insurers also may call upon forensic investigation experts – beyond the experts working directly with the insured – to advise them in connection with "related claims" issues.

The investigation of one data breach often leads to the discovery of another. As these investigations often take place over a limited time period, organizations may discover multiple data breaches (or multiple pieces of the same breach) in a short period of time. These situations require insurers and policyholders to carefully analyze "related claims" language and the specific facts and circumstances at issue. While there have been no reported decisions addressing related claims in the context of cyber insurance policies, the law in other areas is well developed, and courts will likely look to those precedents for guidance in resolving complex coverage questions. ■

For more information, please contact:

Marc E. Rindner
202.719.7486
mrindner@wileyrein.com

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Bonnie T. Wise
202.719.3763
bwise@wileyrein.com

'"Relatedness' Issues Under Cyber Insurance Policies" was first published in the Third Quarter 2017 *PLUS Journal*, found **here**.

Draft IoT Legislation Increases Obligations on Contractors and Promotes Vulnerability Disclosure *continued from page 5*

companies selling connected products to the government to make commitments about security and expand support. Certifications about security could open the door to additional liability for contractors under the False Claims Act. And the law would encourage more research and "hacking" of products provided to the government, increasing burdens on the private sector when dealing with the federal government and depriving them of choice in whether and how to manage vulnerability disclosure.

The law would create new contractor responsibilities with respect to Internet-connected device security. The legislation directs the Office of Management and Budget (OMB) to create guidance to federal agencies to include contract provisions for the acquisition of Internet-connected devices. All contracts for the acquisition of Internet-connected devices (devices) will include a clause requiring the contractor to certify that the devices do not contain, at the time of proposal, any known "security vulnerabilities" in any hardware, software, or firmware component. The clause will also require the contractor to certify that the device relies on components capable of accepting properly authenticated and trusted updates from the vendor, and uses only "non-deprecated industry-standard protocols and technologies" for functions such as communications, encryption, and interconnection with other devices or peripherals. Finally, the clause requires the

continued on page 8

contractor to certify that the device does not include any fixed or hard-coded credentials or passwords used for remote administration, delivery of updates, or communication.

All contracts for IoT devices will also include clauses requiring the contractor to: (1) notify the purchasing agency of any known security vulnerabilities or defects subsequently disclosed to it or otherwise learned, for the duration of the contract; (2) update or replace any software or firmware; (3) timely repair any new security vulnerability, or replace, if an update does not remedy the issue; (4) provide the purchasing agency with general information on the device to be updated, relating to the anticipated support and manner in which the device receives updates.

The law would create guidelines for each agency to impose coordinated disclosure requirements on contractors providing Internet-connected devices. The U.S. Department of Homeland Security is to issue guidelines for coordinated vulnerability disclosure requirements for federal contractors supplying IoT devices to the government. These guidelines include policies and procedures for conducting research on the cybersecurity and potential vulnerability of a device. The law would also amend the Computer Fraud and Abuse Act (CFAA) and Digital Millennium Copyright Act (DMCA) to limit liability for those in "good faith" engaging in researching the cybersecurity of a type of device provided by a contractor to the government, and acting in compliance with the National Protection and Programs Directorate's promulgated guidelines. To facilitate this research and disclosure, the law would require OMB to establish, maintain, and update a public database of devices and manufacturers (1) for which limitations of liability exist under the Act, and (2) about which the government has received formal notification of security support ending.

As we have noted elsewhere, vulnerability disclosure programs can be complex and require careful consideration and resources to properly execute. *See* **Considering a Vulnerability Disclosure Program? Recent Push Raises Questions for General Counsel**, *CircleID* (Feb. 10, 2017). There, Megan Brown and Matthew Gardner explain that not every company can handle one. It should be a company's choice whether to have one and whether to waive their rights under the CFAA and DMCA. Finally, it is not necessarily the best approach to address vulnerabilities in devices used by the federal government. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Moshe B. Broder
202.719.4186
mbroder@wileyrein.com

Events & Speeches

Clinical Genomics at WU and Current Challenges for Precision Medicine

Kirk J. Nahra, Moderator & Speaker

Washington University in St. Louis Institute for Policy in Medicine & Law Planning Symposium

September 18, 2017 | St. Louis, MO

The Fundamentals of Incident Response

Megan L. Brown, Speaker

12th Annual ABA Homeland Security Law Institute

September 25, 2017 | Washington, DC

The "S" in IoT Stands for Security

Megan L. Brown, Moderator

U.S. Chamber of Commerce's Sixth Annual Cybersecurity Summit

October 4, 2017 | Washington, DC

Cybersecurity & Data Privacy Breakfast & Business Cards

Megan L. Brown, Speaker

William & Mary Alumni Event

October 5, 2017 | Washington, DC

Managing Data Security Contracts and Multiple Obligations

Kirk J. Nahra, Speaker

2017 Privacy & Security Forum

October 4-6, 2017 | Washington, DC

Privacy Bootcamp for Security Professionals

Kirk J. Nahra, Speaker

IAPP's Privacy. Security. Risk. 2017 Conference

October 16, 2017 | San Diego, CA

I'm a Lawyer: How Can I Advise on Data Security Issues?

Kirk J. Nahra, Speaker

IAPP's Privacy. Security. Risk. 2017 Conference

October 17, 2017 | San Diego, CA

Security @ San Francisco 2017

Matthew J. Gardner, Speaker

HackerOne

October 24, 2017 | San Francisco, CA

U.S. Chamber of Commerce 2017 Legal Reform Summit: The Litigation Jungle

Megan L. Brown, Speaker

October, 25, 2017 | Washington, DC

Health Care Delivery and Payment Reform: Global Payment and Measurement

Kirk J. Nahra, Moderator

AUWCL and ASLME Presents: Next Steps in Health Reform 2017

October 26, 2017 | Washington, DC

Megan Brown Named a 'D.C. Rising Star' by *The National Law Journal*

Megan L. Brown, a partner in Wiley Rein's Appellate, Litigation, Privacy & Cybersecurity, and Telecom, Media & Technology practices, was named a "D.C. Rising Star" by *The National Law Journal*, which selected 40 of D.C. metro area's top lawyers under age 40 across a comprehensive range of practices. Ms. Brown was the only honoree noted for practicing in the areas of technology, litigation, and regulatory.

In selecting the list, the publication's editors looked for "key elements, including success on the highest stages" by lawyers who work in some of the "most sophisticated practices in the nation."

Ms. Brown handles complex litigation and regulatory proceedings for blue-chip wireless, Internet, and technology clients, and shapes the law on privacy, cybersecurity, and the Internet of Things. A former senior U.S. Department of Justice official in the George W. Bush administration, Ms. Brown is well-positioned to help clients navigate the current administration.

The profile of Ms. Brown can be found **here** (subscription required).

Contributing Authors

Moshe B. Broder	202.719.4186	mbroder@wileyrein.com
Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
John T. Lin	202.719.3570	jlin@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Marc E. Rindner	202.719.7486	mrindner@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com
Bonnie T. Wise	202.719.3763	bwise@wileyrein.com