Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | October 2015

Introduction

We continue our focus on litigation this month, with a series of articles highlighting some important new decisions.

First, however, we spend some time on the biggest privacy development of the past few weeks (and maybe for much longer), the drastic changes to the Safe Harbor environment for EU data transfers to the United States. Amy Worlton and Umair Javed look at the recent decision invalidating the Safe Harbor, and assess the initial changes for this landscape. We'll be watching this issue closely over the coming months—let us know if we can help you assess your options.

On the litigation front, we look at some important decisions related to an increasingly important element of the overall privacy/security universe—the role of insurance coverage (and the limitations of such coverage). Laura Foggan and Edward Brown assess the *Urban Outfitters* decision from the Third Circuit holding that a series of insurance policies did not provide coverage for lawsuits involving a retailer's alleged practices in collecting ZIP codes at point of sale in credit card transactions. They also review the *Defender Security* case from the Seventh Circuit dealing with coverage issues for a claim related to the secret recording of telephone calls. Lastly, they also look at the recent *Aspen Way Enterprises* decision from Montana, addressing coverage for claims related to spyware. You can also see a brief summary and a link to a recent podcast I did with law professors Nick Terry and Frank Pasquale for their "The Week In Health Law" series, addressing a wide variety of "hot topics" involving privacy and security in the health care industry.

As always, please let me know if we can be of any assistance on these issues, or if you have other topics you would like us to address in *Privacy In Focus*. I can be reached at 202.719.7335 or knahra@wileyrein.com. ■

Kirk Nahra, Privacy Practice Chair

Guidance for U.S. Businesses After the Historic Safe Harbor Decision

On October 6, 2015, in a landmark decision with far-reaching consequences for both U.S. and European businesses, the Court of Justice of the European Union (CJEU) ruled that the EU-U.S. Safe Harbor Agreement is invalid. For companies relying on the Safe Harbor to transfer EU personal data to the United States, the decision means that they will either need to find a data transfer work-around, localize their data within the EU, or risk being technically out of compliance. Although many companies seem to be prepared with a work-around, there has been understandable confusion since the CJEU's historic ruling about what happens next and whether there is any legal and practical way forward on EU/U.S. data flows. Indeed, the European Parliament's Civil Rights Committee (LIBE) has called for reflection on how the CJEU's judgment affects other ways of transferring data, and at least one EU Member State data protection commissioner already has declared that U.S. businesses should do a complete review of their data transfers and consult with him in every instance.

continued on page 2

ALSO IN THIS ISSUE

Guidance for U.S. Businesses After the Historic Safe Harbor Decision *continued from page 1*

One thing is clear: a political solution is needed to settle uncertainties and avoid the potential legal patchwork created by the CJEU's decision.

The EU-U.S. Safe Harbor Framework

Until recently, the EU-U.S. Safe Harbor Framework provided a method for U.S. companies to transfer personal data outside the EU in a manner consistent with the EU Data Protection Directive (Directive). The Directive is the EU's comprehensive data privacy law, adopted in 1995. Officially titled the "European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," the Directive seeks to "protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of data" and to facilitate the "free flow of personal data" among EU member states by harmonizing privacy laws across the EU. With this broad objective as a springboard, the Directive extensively regulates the processing of personal data in the EU, imposing rules that break down into three categories: (1) complying with certain data quality principles and rules; (2) disclosing to data subjects and addressing their concerns; and (3) reporting to state agencies. One of the most important aspects of the Directive, however, is its restrictions on cross-border data transfers. Transfers of personal data to countries outside the EU are permissible only if the recipient country "ensures an adequate level of protection." Only a handful of countries have been found to meet this standard. Notably, the U.S. is not one of them.

For this reason, the Directive immediately presented a serious threat to the flow of data between the EU and the U.S. Regulators in the EU and the U.S. recognized the threat, however, and fashioned the Safe Harbor as a solution. Formally adopted on July 26, 2000, the Safe Harbor has been a voluntary self-certification program for transmitting data from the EU to the U.S. under the Directive. Specifically, under the program, U.S. companies have lawfully received personal data from Europe once they publicly agreed to treat the data according to the Safe Harbor Principles, which resemble EU data privacy laws. Self-certification was made to the U.S. Department of Commerce. The advantages of the Safe Harbor for participating U.S. companies have included broad protection from EU regulators, EU courts, and EU law. Safe Harbor compliance instead has been enforced by the U.S. Federal Trade Commission (FTC) pursuant to U.S. statutory authority. The Safe Harbor agreement permits limitations to data protection rules where necessary on grounds of national security, public interest, or law enforcement requirements. As of the date of the CJEU's ruling, more than 4,000 U.S. companies had membership in the Safe Harbor.

Criticism of the Safe Harbor and Safe Harbor 2.0

Criticism of the Safe Harbor is nothing new. The Safe Harbor has attracted criticism since its approval in 2000, and European regulators ramped up those criticisms in the wake of the Snowden disclosures regarding U.S. national security surveillance activities. As details of U.S. surveillance activities emerged, European officials increasingly called for review and, in some cases, suspension of the agreement. In fact, the European Commission released a six-point action plan in 2013 to restore trust in data flows between the U.S. and the EU. The plan, among other considerations, contemplated accelerated review of a proposed EU data protection reform package as well as the extension of certain U.S. privacy protections to EU citizens. The plan preserved the Safe Harbor framework despite criticism in the EU, and regulators on both sides of the Atlantic have since been negotiating "Safe Harbor 2.0" to address EU concerns about the data sharing pact. Although those negotiations reportedly were nearing completion, Safe Harbor 2.0's status now is unclear in light of the CJEU's ruling.

The Challenge: *Schrems v. Data Protection Commissioner*

In *Schrems v. Data Protection Commissioner*, Austrian law student Max Schrems filed an outright legal challenge to data transfers to the U.S. Schrems filed a complaint with the Irish Data Protection Commission (DPC) claiming that "the law and practices of the United States offer no real protection of the data kept in the United States against State surveillance." Schrems' complaint related to his use of Facebook and Facebook's transfer of EU personal data to the U.S.

The Irish DPC initially declined to investigate, concluding that the Safe Harbor principles were dispositive. The case was appealed to the High Court of Ireland, which asked the CJEU to decide two questions:

- Whether a data protection commissioner is bound by a [European Commission] finding that the Safe Harbor agreement provides adequate protection in the face of a complaint alleging it does not; or, alternatively,

continued on page 6

Third Circuit Finds No CGL Coverage for Claims Challenging Retailer's Collection of Customer ZIP Codes

The U.S. Court of Appeals for the Third Circuit, applying Pennsylvania law, has held that a series of Comprehensive General Liability (CGL) and umbrella policies did not afford coverage for three lawsuits against a retailer in connection with the retailer's alleged practices in collecting ZIP codes at point of sale in credit card transactions and then using the data for promotional purposes. *See OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc.,* 2015 U.S. App. Lexis 16399, No. 14-2976 (3d Cir. Sept. 15, 2015).

Prior Proceedings

The policyholder, a clothing retailer, was sued in three underlying putative class action lawsuits alleging that it violated a number of state statutes and customers' common law privacy rights in connection with the retailer's practices at point of sale. After the policyholder sought coverage for those suits from two insurers that had issued it CGL and umbrella policies, one of the insurers filed a declaratory judgment action seeking a determination that it had no duty to defend or indemnify the policyholder in the three underlying suits. The policyholder, in turn, joined the second insurer as a third-party defendant.

The policies at issue afforded coverage for "personal and advertising injury," which was defined to include an injury arising out of "oral or written publication [, in any manner,] of material that violates a person's right of privacy." The policies also contained identical exclusions for "'personal and advertising injury' arising directly or indirectly out of any action or omission that violates or is alleged to violate … [any] statute, ordinance or regulation … that addresses, prohibits or limits the … dissemination, … collecting, recording, sending, transmitting, communicating or distribution of material or information." The district court ruled in favor of the insurers, holding that none of the suits were covered by the relevant policies.

A discussion of the district court ruling, as well as its implications, can be found here.

Third Circuit Decision

On appeal, the Third Circuit affirmed. Regarding the first lawsuit, the court ruled that coverage was not triggered because the suit did not allege a "publication." In so ruling, the court noted that the lawsuit focused on allegations that the retailer requested and collected customer ZIP codes and then used those ZIP codes for its "own pecuniary benefit, including by engaging in direct marketing campaigns … by matching the customers' names with their ZIP codes to identify the customers' home/business address via commercially available databases." The court ruled that there was no "publication" because there had been no "dissemination [of information] to the public at large" alleged in the underlying suit, and as a result, that coverage was not triggered in the first instance.

The court next ruled that the second lawsuit, which involved a single cause of action for violations of the Song-Beverly Credit Card Act of 1971 following the dismissal of various other claims, was not covered by the policies either. In so ruling, the court applied an exclusion barring coverage for "'[p]ersonal and advertising injury' arising directly or indirectly out of any action or omission that violates or is alleged to violate … [a]ny federal, state or local statute, ordinance or regulation … that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information." In holding that the exclusion squarely applied, the court rejected the policyholder's argument that the same allegations supporting the Song-Beverly Credit Card Act count could also support common law claims.

Finally, the court ruled that a third lawsuit, which alleged that the defendants "engage[d] in a practice of 'collecting ZIP codes at checkout at its … stores from customers who make purchases with Credit Cards, recording that information as part of the Credit Card transaction, and then using that information for its own marketing and promotional purposes, including to send unsolicited marketing and promotional materials, or 'junk mail,'" did not trigger coverage. The court ruled that the "right to privacy" at issue in those allegations was the right to "seclusion" (protecting an interest to be free from unsolicited commercial contacts), whereas the "right to privacy" covered under the personal and advertising injury coverage section of the policies was the right to "secrecy" (an interest in keeping data secret). Here, because the allegations in the underlying complaint only implicated the right to seclusion (not an interest in keeping their ZIP codes secret), the court ruled that the complaint allegations did not trigger coverage under the policy.

The Decisional Trend

The Third Circuit's *Urban Outfitters* ruling is consistent with a growing number of decisions that have declined to find general liability coverage for consumer claims concerning "privacy" and

continued on page 7

Seventh Circuit: No "Publication" in Unlawful Recording of Telephone Calls

The U.S. Court of Appeals for the Seventh Circuit, applying Indiana law, has held that an underlying lawsuit alleging that a policyholder secretly recorded phone calls during which customers provided sensitive personal information did not trigger coverage under the personal and advertising injury coverage section of a Comprehensive General Liability (CGL) policy because the recording of information did not constitute "publication." *See Defender Sec. Co. v. First Mercury Ins. Co.*, 2015 U.S. App. Lexis 17116; No. 14-1805 (7th Cir. Sept. 29, 2015).

Judicial Proceedings

The policyholder, a seller of home security systems, was sued in a putative class action alleging that it recorded phone calls from customers without first notifying them and/or obtaining their permission. The named plaintiff also alleged, among other things, that she provided personal information, such as her full name, address, date of birth, and social security number, during the phone call. The lawsuit alleged that the policyholder's conduct violated California Penal Code § 632, which prohibits the recording of confidential telephone communications without the consent of all parties, and § 632.7, which does the same for communications made from a cellular or cordless phone.

The policyholder tendered the suit under its CGL policy, which afforded "personal and advertising injury" coverage for injuries "arising out of … [o]ral or written publication of material that violates a person's right of privacy." The insurer refused to defend, however, and the policyholder subsequently brought suit alleging breach of contract and bad faith. The district court granted the insurer's motion to dismiss, holding that the lawsuit did not trigger coverage in the first instance, because the complaint did not allege facts showing that the injury arose from a "publication." The policyholder appealed.

On appeal, the Seventh Circuit affirmed the decision in favor of the insurer. In so doing, the court, applying Indiana Law, ruled that the plain meaning of the term "publication," as used in the policy, was not so broad as to encompass the mere unlawful recording of information. The court reasoned that because there was no allegation that the information conveyed to and recorded by the policyholder was ever accessed by or shared with a third party, it was not "published," and thus could not trigger coverage.

Limits of Coverage

The Seventh Circuit's decision in *Defender Security* is an important reaffirmation of the limits of personal and advertising injury coverage under CGL policies. It illustrates that that coverage is limited to certain enumerated torts, and that claims involving the internal misuse of customer data—short of sharing that information with third parties—will not trigger coverage.

Indeed, in September alone, two federal appellate courts and one federal district court ruled that "personal and advertising injury" coverage was not triggered by internal misuse of confidential data. In addition to Defender Security, see the stories in this issue on *OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc.*, No. 14-2976 (3d Cir. Sept. 15, 2015) (collection and misuse of ZIP code information did not trigger coverage because there was no publication); and *Am. Econ. Ins. Co. v. Aspen Way Enters., Inc.*, No. 1:14-00009-SPW (D. Mont. Sept. 25, 2015) (collecting and retaining customers' private data in violation of the Washington Consumer Protection Act and the Washington Computer Spyware Act did not trigger coverage because there was no publication). These rulings join other state and federal decisions similarly recognizing the limits of such coverage. *See, e.g.*, *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 115 A.3d 458 (Conn. 2015) (no "publication" where there was no proof that a third party accessed confidential information on data tapes); *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, 444 Fed. App'x 370, 375-76 (11th Cir. 2011) (the phrase "publication, in any manner" was unambiguous and did not apply when there was no dissemination of information to the public); *Ticknor v. Rouse's Enters., LLC*, 2 F. Supp. 3d 882, 896 (E.D. La. 2014) (in order for "publication" to occur, the material must be "made generally known, announced publicly, disseminated to the public, or released for distribution"). ■

For more information on these decisions or the trends in CGL policy coverage litigation, please contact:

Laura A. Foggan
202.719.3382
lfoggan@wileyrein.com

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Court Finds No Coverage for Spyware Claims

Judge Susan P. Watters of the U.S. District Court for the District of Montana, applying Montana law, has ruled on questions concerning the application of personal and advertising injury coverage in Comprehensive General Litigation (CGL) policies to claims arising from the use of computer software that allegedly captured private data remotely from computers rented or sold to consumers.

Judge Watters held that a lawsuit filed by a state government alleging that a policyholder used software to "collect information on consumers" and "collect private computer activity while consumers were unaware of the activities being recorded" did not allege any "publication" and thus did not trigger personal and advertising injury coverage. *Am. Econ. Ins. Co. v. Aspen Way Enters., Inc.*, 2015 US Dist. Lexis 129274, No. 1:14-00009-SPW (D. Mont. Sept. 25, 2015). In addition, the court ruled that a different lawsuit filed by private litigants and alleging that the policyholder violated the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2511 by "intentionally collecting, transmitting, storing and disclosing, or endeavoring to disclose, to any other person," certain private and confidential information triggered coverage in the first instance but coverage was barred by a "recording and distribution" exclusion in the relevant policies.

Litigation Background

The policyholder was a franchisee that owned and operated rent-to-own stores in Montana, Washington, and Wyoming. During the relevant time period, the policyholder installed software into computers rented or sold to customers. That software, which was activated remotely, enabled the stores to secretly take photographs with the computer's webcam, capture keystrokes, and take screen shots. Once those photographs, keystroke captures, and/or screen shots were taken, the software designer would email the data to the store that activated the software (in this case, the policyholder).

The policyholder's use of the software led to several legal actions against it. First, the policyholder faced a private class action lawsuit by plaintiffs who claimed that the policyholder and other franchisees received private and confidential data after activating the software. After a number of counts in that lawsuit were dismissed, the only remaining claim was for violation of the ECPA, and the plaintiffs alleged that the policyholder violated that statute by "intentionally collecting, transmitting, storing and disclosing, or endeavoring to disclose, to any other person," the contents of private data collected by the software.

Second, the policyholder was sued by the State of Washington, which alleged that the policyholder violated Washington's Consumer Protection Act and Computer Spyware Act by installing the software on customers' computers.

The policyholder sought coverage under a number of general liability insurance policies, and a coverage action involving multiple insurers and the policyholder followed. The court granted summary judgment in favor of the insurers, holding that their policies did not afford coverage for either of the underlying suits.

The Court's Analysis

First, with respect to the private party class action, the court ruled that the suit alleged "oral or written publication, in any manner, of material that violates a person's right of privacy" and thus triggered the personal and advertising injury coverage sections of the relevant policies. The court reasoned that that coverage was triggered because the operative complaint alleged that the plaintiffs' private information was collected by the software installed on their computers and that it had "been repeatedly transmitted via unencrypted email and forwarded to unknown persons and locations." However, each policy contained a "recording and distribution" exclusion, which barred coverage for any suit that alleged a violation of a federal statute that prohibits the transmitting or distribution of material or information. The court applied that exclusion and held that there was no coverage for the private suit because the only count remaining in the action was for violation of the ECPA, which is a federal statute prohibiting the disclosure or use of intercepted electronic communications. On that basis, the court ruled that none of the policies afforded coverage for the private party class action suit.

The court also found no coverage for the lawsuit brought by the State of Washington. The court ruled that the suit did not trigger "personal and advertising injury" coverage because it did not allege "publication." Instead, said the court, the complaint alleged that the policyholder violated Washington state law by collecting and retaining customers' private data in violation of the Washington Consumer Protection Act and the Washington Computer Spyware Act. The court noted that, although one count was titled "Unfair Collection and Disclosure of Private and Confidential Information," the complaint did not allege any "disclosures" but instead focused on the policyholder's use of the software to "collect

continued on page 8

- May and/or must the commissioner conduct an independent investigation of the matter in light of the factual developments since the Safe Harbor agreement was first published.

Schrems was heard by the CJEU in May of this year, and the non-binding opinion of Advocate General Bot was issued on September 23, 2015. The Advocate General's opinion recommended that the CJEU find the Safe Harbor invalid in light of perceived indiscriminate U.S. government surveillance activities.

The CJEU's Ruling

The CJEU issued its judgment on October 6, 2015, a mere 12 days after the Advocate General's opinion was released. The judgment comprised two findings. First, the CJEU found that the Safe Harbor did not eliminate or reduce the powers granted to national data protection authorities (DPA) under the Directive. Accordingly, DPAs have the power to investigate and suspend transfers of personal data to a country outside the EU, even where the European Commission has adopted a finding that the recipient country affords an adequate level of data protection. Second, the CJEU held in unequivocal terms that the Safe Harbor Decision is invalid. The CJEU stated that the access to EU data afforded to the U.S. intelligence community impermissibly interferes with the right to respect for private life and the right to protection of personal data, which are guaranteed under the Charter of Fundamental Rights of the European Union. The CJEU further emphasized that the U.S. does not provide EU citizens with the ability to obtain judicial redress in the U.S. Notably, the CJEU did not find that Facebook itself had violated the Safe Harbor or that it improperly handled EU personal data—the decision instead was grounded in U.S. government activities.

Guidance for U.S. Companies

The Safe Harbor is invalid, which means it no longer can provide a basis for transferring personal data from the EU to the U.S. U.S. companies should complete an audit of their data transfers to identify transfers that were undertaken in reliance of the Safe Harbor. To the extent they have not done so, companies should explore other mechanisms to support ongoing transfers.

Alternative data transfer mechanisms may include the following:

Derogations from Adequacy Requirements. The Directive currently provides a number of derogations from the adequacy requirements for cross-border data transfers. Pursuant to these derogations, a company may transfer EU personal data to the U.S. in the following circumstances: the data subject has given unambiguous consent to the proposed transfer; the transfer is necessary for the performance of a contract between the data subject and the data controller (defined as the party responsible for determining how to collect, store, and otherwise use personal data); the transfer is necessary for the performance of a contract concluded in the interest of the data subject; the transfer is legally required; or the transfer is necessary in order to protect the vital interests of the data subject. However, companies should be careful about relying on these provisions to justify data transfers, as they are subject to narrow interpretations by EU DPAs.

Model Contract Clauses. Model contract clauses likely are the best short-term solution for companies seeking to continue their data transfers. These contractual provisions have been approved by the European Commission. In many ways, however, they are stricter than the requirements of the Safe Harbor. In addition, in some cases, they require pre-approval from national data protection authorities and expose U.S. companies to EU regulators and EU legal actions.

Binding Corporate Rules (BCRs). BCRs allow companies to develop and adopt internal privacy policies that mandate EU-style data protections across the entire organization. Adopting BCRs is a time-consuming and expensive undertaking, generally requiring consultation and consensus with multiple EU DPAs. Thus, BCRs do not present an immediate solution for U.S. participants in the Safe Harbor. They may, however, present a longer-term solution for companies that are seeking a global solution for exports of EU personal data or a custom solution for trans-Atlantic data flows.

Data Anonymization. If the data transferred to the U.S. need not be in an identifiable format, companies could consider anonymizing the data. Companies should note, however, that EU rules set a high bar for anonymization.

Caution is warranted, however, as the CJEU's reasoning in *Schrems* could allow EU DPAs to challenge the viability of these alternative methods as well. In fact, a proclamation issued by LIBE calls for reflection "immediately" on how the judgment affects other ways of transferring data, including model contractual clauses and BCRs. In addition, a German data protection commissioner has recommended that companies using model contractual clauses cancel

continued on page 7

Guidance for U.S. Businesses After the Historic Safe Harbor Decision *continued from page 6*

them and consult with him on each data transfer. Other DPAs may soon follow suit.

Next Steps

The CJEU's ruling has created legal and practical uncertainties between the two largest trading partners in the world that need to be resolved as soon as possible. Indeed, the decision paves the way for national DPAs to challenge any adequacy finding and any transfer, regardless of the data transfer mechanism. The result could be a regulatory nightmare for companies that, going forward, may be required to ensure compliance with fragmented data protection rules across 28 EU jurisdictions. The decision also raises questions as to the status of data previously transferred under the Safe Harbor.

The European Commission has promised guidance on how to deal with data transfers to the U.S., and there already has been a meeting between the Commission and national DPAs. While there has been no official statement from that meeting yet, a second meeting was held on October 15. Businesses should consider reaching out to U.S. and European policymakers to push for the development of reliable legal mechanisms for maintaining data flows and harmonization of privacy rules across the EU.

In the meantime, companies that have certified their compliance to the Department of Commerce under the Safe Harbor should continue to fulfill their privacy commitments under the Agreement. An organization's self-certification of compliance with the EU-U.S. Safe Harbor Framework constitutes an enforceable representation to the Department of Commerce and the public that it adheres to a privacy policy that complies with the EU-U.S. Safe Harbor. A company that acts contrary to those commitments could expose itself to enforcement by the FTC for "unfair or deceptive acts or practices" under its Section 5 authority. ■

For more information, please contact:

Amy E. Worlton
202.719.7458
aworlton@wileyrein.com

Umair Javed
202.719.7475
ujaved@wileyrein.com

Third Circuit Finds No CGL Coverage for Claims Challenging Retailer's Collection of Customer ZIP Codes *continued from page 3*

policyholder handling of data containing personally identifiable information. Thus, a number of courts specifically have recognized limits on the meaning of the CGL Coverage B offense of "publication" of material that violates a person's right to privacy. *See, e.g.*, *Whole Enchilada, Inc. v. Travelers Prop. Cas. Co. of Am.*, 581 F. Supp. 2d 677, 697 (E.D. Pa. 2008); *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, 444 Fed. App'x 370 (11th Cir. 2011). Further demonstrating that CGL policies will not broadly respond to privacy claims, in the first high court decision to address coverage under a CGL policy for data breach claims, the Connecticut Supreme Court recently held that the personal and advertising injury coverage section did not afford coverage. *See Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 115 A.3d 458 (Conn. 2015).

Urban Outfitters is an important ruling directly addressing whether CGL and umbrella insurance coverage may respond to a suit alleging improper gathering and use of ZIP code information. Wiley Rein LLP will continue to follow litigation over whether and to what extent insurance coverage responds to such suits. ■

For more information, please contact:

Laura A. Foggan
202.719.3382
lfoggan@wileyrein.com

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Court Finds No Coverage for Spyware Claims *continued from page 5*

information on consumers" and to "collect private computer activity while consumers were unaware of the activities being recorded." As such, the court ruled that the government lawsuit did not trigger coverage in the first place.

This case is illustrative of the growing body of case law rejecting coverage under the personal and advertising injury coverage sections in CGL policies for certain privacy-related claims. For example, earlier this month, the Third Circuit Court of Appeals held that three different lawsuits arising from a retailer's alleged improper collection and use of ZIP code information in violation of a state statute prohibiting such conduct were not covered under a series of CGL and umbrella policies. *See the story in this issue on* *OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc.*, No. 14-2976 (3d Cir. Sept. 15, 2015).

Aspen Way Enters., Inc. is significant because of the court's refusal to disregard the "publication" element necessary to trigger personal and advertising injury coverage. Here, the policyholder argued that the allegations of improper collection and retention of customers' private data, combined with the title to one of the counts alleging "Unfair Collection *and Disclosure* of Private and Confidential Information" (emphasis added), was enough to trigger coverage. The court disagreed, observing that there is a distinction between "collection" or "use," on the one hand, and "publication," on the other. Likewise, although the court ultimately determined that the private party class action lawsuit's allegations were sufficient to trigger coverage (but ruling for the insurers on the basis of an exclusion), it noted that the information was shared between the software developer, the retailer, and other "unknown persons and locations" in unencrypted form. Thus, in a case where there is no transfer of information to a third party, or if the information is in encrypted form and there is no evidence of access to that information, the court might well find the "publication" element not satisfied. *See Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 115 A.3d 458 (Conn. 2015) (no "publication" where there was no proof that a third party accessed confidential information on data tapes). ■

For more information, please contact:

Laura A. Foggan
202.719.3382
lfoggan@wileyrein.com

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Listen to Kirk Nahra's October 2 Podcast

Kirk Nahra was featured on "The Week in Health Law" podcast hosted by Indiana University Professor of Law Nicholas P. Terry and University of Maryland Professor of Law Frank Pasquale. The 45-minute podcast is available for free here.

In response to the professors' questions, Kirk provided his perspective on the implications of the U.S. Court of Appeals for the Third Circuit's *Wyndham* decision, class actions arising from data breaches, possible additions to the HIPAA regulations, future regulation of personal information in the "HIPAA-free zone," threats to EU-U.S. data exchange, and privacy implications of the House-passed 21st Century Cures Act, among other matters.

Kirk J. Nahra can be reached at 202.719.7335 or knahra@wileyrein.com

SPEECHES & EVENTS

Future Trends in Privacy and Security – Policy Session

Kirk J. Nahra, Speaker

Privacy and Security Forum

October 21-23, 2015 | Washington, DC

The Telephone Consumer Protection Act... Stuck in the 1990's

Scott D. Delacourt, Panelist

U.S. Chamber of Commerce Institute for Leaw Reform Panel

October 22, 2015 | Washington, DC

continued on page 9

Risk-Informed Regulation

Anna M. Gomez, Moderator

Silicon Flatirons Center Conference: Risk Assessment in Spectrum Policy

October 23, 2015 | Boulder, CO

Coverage for Data Breaches Under Traditional Insurance Policies and Introduction to Cyber Policies

Laura A. Foggan, Speaker

DRI Seminar: Data Breach and Privacy Law

November 4 - 6, 2015 | Chicago, IL

Coverage for Data Breaches Under Traditional Insurance Policies and Introduction to Cyber Policies

Edward R. Brown, Speaker

DRI Seminar: Data Breach and Privacy Law

November 5, 2015 | Chicago, IL

FTC: Dictator? Collaborator? Facilitator?

Kirk J. Nahra, Speaker

IAPP Practical Privacy Series 2015: FTC and Consumer Privacy

November 18, 2015 | Washington, DC

Coverage Issues Arising from Cyber Security Breaches

Laura A. Foggan, Speaker

DRI Insurance Coverage and Practice Symposium

December 3 - 4, 2015 | New York, NY

Here's the Thing: Physical Harms from Cyber Perils - Are They Covered?

Laura A. Foggan, Speaker

ABA's 2016 Insurance Coverage Litigation Committee CLE Seminar

March 3, 2016 | Tucson, AZ

What's Next for Health Care Privacy?

Kirk J. Nahra, Speaker

Twenty-Fourth National HIPAA Summit

March 21-23, 2016 | Washington, DC

The Changing Face of Health Care Privacy

Kirk J. Nahra, Speaker

Global Priavy Summit 2016

April 3-6, 2016 | Washington, DC

Contributing Authors

Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Laura A. Foggan	202.719.3382	lfoggan@wileyrein.com
Umair Javed	202.465.7475	ujaved@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Amy E. Worlton	202.719.7458	aworlton@wileyrein.com