Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | February 2016

Introduction

This month, the focus stays on the key developments in Europe, and some important developments in the growing law of cybersecurity. Amy Worlton and Umair Javed describe the recent developments concerning the developing "Privacy Shield," the proposed framework to replace the now defunct Safe Harbor scheme. This program – still being developed – will be enormously important for any company with data transfer issues out of Europe. Megan Brown, Nova Daly, and Matt Gardner describe the recent White House initiatives related to cybersecurity, as well as the announcement of the new Federal Privacy Council. Megan and Jeremy Broggi also discuss the upcoming proposals from the Department of Homeland Security to re-evaluate the Protected Critical Infrastructure Information regulations. Laura Foggan and Ted Brown continue their series on the growing law of insurance coverage related to cybersecurity and privacy issues, discussing the insurance elements of a recent decision involving an allegedly unlawful posting of genetic information.

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

– Kirk Nahra, Privacy Practice Chair

Is the 'Privacy Shield' a New Foundation for EU-U.S. Data Flows?

On February 2, the European Commission and the United States government announced an 11th hour agreement in principle to replace the invalidated Safe Harbor, which previously allowed lawful transfers of personal data between the European Union (EU) and the United States. Throwing the legality of trans-Atlantic personal data flows into upheaval, the Court of Justice of the European Union (CJEU) struck down the Safe Harbor in October 2015, finding in part that access to EU personal data afforded to the U.S. intelligence community impermissibly interfered with EU citizens' privacy rights. In response to the CJEU ruling, EU data protection authorities (DPAs) called on EU Member States, EU institutions, and the U.S. government to "find political, legal and technical solutions enabling data transfers" by the end of January 2016, or risk coordinated enforcement actions.

U.S. and EU negotiators have announced agreement on the broad outlines of a plan to replace the Safe Harbor, but many challenges and risks remain. Few details about the new agreement, which is being called the EU-U.S. Privacy Shield, have been released. U.S. companies therefore have little insight into what their privacy obligations might be, should they choose to use the Privacy Shield. On the other side of the Atlantic, some EU DPAs already have voiced concerns over whether the Privacy Shield adequately protects EU citizens' privacy rights, or whether it is simply a repackaged Safe Harbor. In fact, a February 3 statement issued by the EU Article 29 Working Party, an advisory group comprised of representatives from EU DPAs, demonstrates that significant uncertainty remains over trans-Atlantic data flows at this time. So, while the agreement is a step forward, U.S. companies should

continued on page 2

ALSO IN THIS ISSUE

remain cautious.

Below, we highlight some key features of the Privacy Shield based on the limited information that has been made available. We also review the Article 29 Working Party statement, which offers some new insight into enforcement risks and the adequacy of alternative data transfer mechanisms, such as model contractual clauses and binding corporate rules. Finally, we discuss next steps for the Privacy Shield, which still faces a long road to adoption.

The EU-U.S. Privacy Shield

According to the European Commission, the Privacy Shield will include the following elements:

Obligations on U.S. companies and enforcement. Under the Privacy Shield, U.S. companies that receive personal data from the EU will be required to commit to "robust" obligations on how that personal data is processed and how individual rights are guaranteed. The U.S. Department of Commerce will require Privacy Shield companies to publish their privacy commitments, which ensures that they are enforceable under U.S. law by the Federal Trade Commission (FTC). U.S. companies handling EU human resources data also will be required to commit to comply with decisions by European DPAs.

So far, these obligations should sound familiar to companies that previously were enrolled in the Safe Harbor, as they are consistent with long-standing practices under that agreement. However, the Department of Commerce has offered some additional detail on where the new agreement diverges from its predecessor. Specifically, the Department of Commerce has indicated that the Privacy Shield will create "new contractual privacy protections and oversight for data transferred by participating companies to third parties or processed by those companies' agents to improve accountability and ensure a continuity of protection." The Department of Commerce also has stated that under the new agreement, it will "step in directly and use best efforts to resolve referred complaints, including by dedicating a special team with significant new resources to supervise compliance with the Privacy Shield."

Safeguards and transparency obligations on U.S. government access. For the first time, U.S. authorities have provided written assurances to the EU that U.S. law enforcement and national security access to EU citizens' personal data "will be subject to clear limitations, safeguards, and oversight mechanisms." Specifically, to address concerns raised in the CJEU ruling, the Privacy Shield will ensure that EU personal data will not be subject to "indiscriminate mass surveillance." Rather, data collections for law enforcement or national security purposes under the new arrangement will be "proportionate" and "only to the extent necessary." The European Commission and the Department of Commerce will conduct an annual joint review of the functioning of the arrangement, which will include a review of national security access. EU DPAs will be invited to participate in those reviews.

Protection of EU citizens' rights with several redress possibilities. In perhaps the most significant break from the Safe Harbor, the Privacy Shield will provide EU citizens several avenues for seeking personal redress in the United States. U.S. companies that receive complaints from EU citizens will have deadlines to respond. European DPAs also will be able to refer complaints directly to the Department of Commerce and the FTC. Finally, the Privacy Shield will offer alternative dispute resolution free of charge and an "ombudsperson" for complaints relating to access by national intelligence authorities. According to the Department of Commerce, Privacy Shield companies also will be required to participate in arbitrations "as a matter of last resort to ensure that EU individuals who still have concerns will have the opportunity to seek legal remedies."

The Article 29 Working Party Statement

EU DPAs comprising the Article 29 Working Party issued a much-anticipated statement on February 3, 2016, the day after EU and U.S. negotiators announced the Privacy Shield deal. The statement "welcomed" the conclusion of negotiations and expressed the Working Party's anticipation for reviewing the specific contours of the Privacy Shield, so that it can assess whether the new agreement can "answer the wider concerns raised by the [CJEU] judgment." To that end, the statement called on the European Commission to make all documents pertaining to the Privacy Shield available for review by the end of February.

A key question remains unresolved in the Article 29 statement—namely, whether the deal extends the unofficial moratorium on enforcement actions. In the United States, FTC Commissioner Julie Brill stated that she understood that European DPAs would not bring enforcement actions against companies until the Privacy Shield is fully in place. This statement may be at odds with the February 3 statement by the Article 29 Working

continued on page 3

Party, which emphasized that U.S. companies no longer can rely on the Safe Harbor for their data transfers from the EU and that "EU data protection authorities will therefore deal with related cases and complaints on a case-by-case basis."

The Article 29 Working Party statement does provide some guidance to U.S. companies by finding that, while it reviews the Privacy Shield, other transfer mechanisms, such as standard contractual clauses and binding corporate rules, still can be used for lawful personal data transfers to the United States. This is not to suggest that the Working Party has fully blessed these alternative data transfer mechanisms—only that its review is ongoing and it has not found them inadequate.

Next Steps

The Working Party has requested that the European Commission deliver all documents on the Privacy Shield by the end of February. The Working Party then will complete its assessment for all personal data transfers to the United States at an extraordinary plenary meeting around the end of March. After this period, the Working Party plans to consider whether alternative transfer mechanisms, such as model contractual clauses and binding corporate rules, still are valid for data transfers to the U.S.

With respect to the Privacy Shield, the European Commission must prepare a draft adequacy decision for the arrangement, which then could be adopted following consultation with a committee of Member State representatives. In the meantime, the United States must prepare to implement the Privacy Shield and formalize its commitments in writing. The European Commission has expressed its expectation that the Privacy Shield can be adopted within three months. Until then, U.S. companies should consider using alternative mechanisms to transfer data to the U.S. and carefully monitor developments.

For more information on these and other data transfer issues, please contact:

Amy E. Worlton
202.719.7458
aworlton@wileyrein.com

Umair Javed
202.719.7475
ujaved@wileyrein.com

POTUS Launches Significant Cybersecurity and Privacy Initiatives

On February 9, President Obama initiated a number of consequential actions on cybersecurity. The initiatives range from establishing by Executive Order a new Federal Privacy Council made up of senior privacy officials from two dozen agencies that will improve federal privacy protections for individuals, to creating a comprehensive Cybersecurity National Action Plan that will encompass a long-term, strategic assessment of cybersecurity in the 21st century.

Several federal agencies also have been looking at and acting on critical issues related to cybersecurity; some appear to be inching toward oversight or regulatory efforts aimed at assessing use or compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Notable components of the President's initiatives include:

- Creating a Commission on Enhancing National Cybersecurity that draws from the private sector to make recommendations by year-end to improve cybersecurity awareness and practices and foster new technologies;
- Funding significant financial investments in government information technology and cybersecurity efforts beginning in the next fiscal year;
- Establishing the Federal Chief Information Security Officer to lead and coordinate the various new programs and efforts; and
- Harnessing private initiatives to help secure personal data online through multi-factor authentication and other methods, to be spearheaded in a new National Cybersecurity Awareness Campaign focused on consumers.

These efforts are further evidence of the urgency with which the government is looking at the private sector's approach to cybersecurity and the operations put in place to safeguard digital information and

continued on page 4

protect against cybersecurity vulnerabilities. The President's actions build on previous Executive Orders like Executive Order 13636, creation of the voluntary Cybersecurity Framework by NIST, and successful passage of the Cybersecurity Enhancement Act of 2014 and the Cybersecurity Information Sharing Act of 2015. In addition, the Office of Management and Budget (OMB) released proposed guidance designed to take "major steps" to improve cybersecurity in federal acquisitions in August 2015.

Important questions remain concerning the implementation of many of these recent federal efforts. NIST is evaluating the use and role of its Cybersecurity Framework in protecting critical infrastructure. The U.S. Department of Homeland Security (DHS) and other agencies are just beginning to implement the terms of The Cybersecurity Act of 2015, and the federal government is trying to improve communication through Information Sharing and Analysis Organizations. We expect one critical program, the Protected Critical Infrastructure Information (PCII) regime, administered by DHS, also to be revisited this Spring. Some states also have expressed interest in private sector cyber preparedness, further complicating the landscape.

In this most recent effort, President Obama is also requiring agencies to identify and prioritize their highest value and most at-risk IT assets and then take additional concrete steps to improve their security. Whether such steps result in procurement obligations or regulation more broadly remains to be seen.

The private sector should follow the progress of these initiatives and related developments to be aware of the government's expectations and their implications for U.S. business, security, and investment.

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Nova J. Daly
202.719.3282
ndaly@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

DHS to Consider Important Changes to Regulations Protecting Voluntarily Shared Critical Infrastructure Information

In the wake of recent congressional action to promote cybersecurity and critical infrastructure information sharing, the U.S. Department of Homeland Security (DHS) is expected soon to reevaluate its approach to a flagship program for protecting critical infrastructure information voluntarily shared with the government by the private sector. Entities that consider sharing—or that might be asked to share—information with the federal government should think about whether to engage with DHS to shape the next phase of this program.

DHS expects to release this April an Advance Notice of Proposed Rulemaking (ANPRM) to open reconsideration and revision of its Protected Critical Infrastructure Information (PCII) regulations. The PCII regulations establish procedures for the receipt, care, and storage of critical infrastructure information voluntarily submitted to DHS by private sector entities. Among other things, the regulations ensure that information submitted through the program is protected from Freedom of Information Act (FOIA) inquiries and similar disclosure requests.

The ANPRM will provide interested parties with an opportunity to provide input to DHS regarding any needed or helpful changes to its PCII regulations. DHS has not yet publicly signaled the scope of proposed revisions. According to the announcement published in the *Unified Agenda of Federal Regulatory and Deregulatory Actions:*

> DHS is initiating this rulemaking process to help it identify how to enhance the PCII regulation more effectively in achieving [sic] its regulatory objectives. DHS believes that after nine years of experience implementing the PCII program, DHS has gained first-hand insight on lessons learned, and that the ANPRM process provides expanded opportunities for the Department to hear and

continued on page 5

consider the views of interested members of the public on their recommendations for program modifications.

This is timely because federal agencies right now are grappling with how to collect information about cybersecurity readiness. The ANPRM is an important part of the overall discussion of cybersecurity because of the central role that DHS's PCII program can play in protecting and promoting the sharing of critical infrastructure information.

Recent enactments by Congress, including the Cybersecurity Act of 2015 and the Cybersecurity Information Sharing Act of 2015, enshrine DHS as the hub of critical infrastructure and cybersecurity information sharing, including through entities like the National Cybersecurity and Communications Integration Center (NCCIC). Provisions in these and other enactments evidence a strong desire by Congress to promote voluntary information sharing, and to strengthen incentives for private sector participation through protections from disclosure and other potential liability. These protections also promote privacy goals by ensuring that consumer data and other information in the hands of private sector entities is not publicly disclosed. The PCII regulations, which are authorized by statute, are an important piece of that congressional agenda. PCII was not the subject of recent legislation, but is an important tool for the government and private sector. DHS can and should ensure that any revisions to its PCII regulations are consistent with the incentives for sharing that Congress has sought to create.

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com
Jeremy J. Broggi
202.719.3747
jbroggi@wileyrein.com

'Personal Injury' Coverage Triggered by Posting of Genetic Data Online

In a unique case involving a professional liability insurance policy, a Texas federal district court, applying Texas law, has held that an insurer had a duty to defend and indemnify a policyholder under the policy's "Personal Injury" coverage in a suit alleging that the policyholder unlawfully posted personal information about claimants on its website. *See Evanston Insurance Co. v. Gene by Gene, Ltd.*, No. H-14-1842, 2016 WL 102294 (S.D. Tex. Jan. 6, 2016). In so ruling, the court held inapplicable an exclusion barring coverage where there is "any other statute, law, rule, ordinance, or regulation that prohibits or limits the sending, transmitting, communication or distribution of information or other material."

The policyholder, the owner and operator of a genetic genealogy website, offered DNA testing kits to its users to allow them to learn more about their ancestry. The policyholder was sued for allegedly publishing DNA test results on its website without obtaining consent from its users, in violation of a state statute. It sought coverage under a professional liability policy, which included coverage for "Personal Injury," defined to include "oral or written publication of material that violates a person's right of privacy." The insurer filed a declaratory judgment action, seeking a declaration that it did not have a duty to defend or indemnify the policyholder in connection with that suit. The policyholder counterclaimed for breach of contract, and it moved for summary judgment.

Summary Judgment Granted

The court ruled that the policy was triggered in the first instance by allegations of the publication of material—the DNA analysis—that allegedly violated a person's right to privacy. The insurer argued, however, that an exclusion barred coverage. In relevant part, that exclusion barred coverage for claims based upon or arising out of any violation of the Telephone Consumer Protection Act, the CAN-SPAM Act of 2003, or "any other statute, law, rule, ordinance, or regulation that prohibits or limits the sending, transmitting, communication, or distribution of information or other material." The insurer argued that the latter part of the exclusion applied because the relevant claim arose out of an alleged violation of a state statute prohibiting transmitting, communicating, or distributing information on a

continued on page 6

person's DNA without his or her consent. The policyholder argued that the exclusion should be read together with other nearby provisions, which barred coverage only for claims arising out of statutes prohibiting unsolicited communications by telephone or email.

The court granted summary judgment in favor of the policyholder, reasoning that the policyholder's reading of the exclusion was reasonable. The court reasoned that the insurer's interpretation of the exclusion would render illusory the Advertising Injury coverage under the policy, which afforded coverage for claims involving "injury … arising out of oral or written publication of material that libels or slanders a person or organization or a person's or organization's products, goods or operations … occurring in the course of the Named Insured's Advertisement." According to the court, claims based on statutes, laws, or regulations for libel or slander would be excluded from coverage under the insurer's reading. Consequently, it ruled that the policyholder's construction of the exclusion was reasonable. As a result, the court also ruled that the insurer breached its contract when it refused to defend and indemnify the policyholder.

Gene by Gene is an interesting case, although it is likely to have limited precedential effect. Indeed, the facts in *Gene by Gene* involve intentional, volitional conduct, and the parties appeared to have conceded that there was "publication"—which in most instances requires actual access by a third party. By contrast, in a typical "hacking" case involving a security breach, the "publication" element is often not satisfied because a policyholder is unable to show that the sensitive information at issue was actually accessed by a third party and/or because any claim concerns failure to provide notice or failure to adequately protect information, not publication of private material. *See, e.g., Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.,* 115 A.3d 458 (Conn. 2015).

For more information on these and related coverage issues, please contact:

Laura A. Foggan
202.719.3382
lfoggan@wileyrein.com

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

SPEECHES & EVENTS

Are You and Your Insurer Connecting on Cyber Risk?

Laura A. Foggan, Panelist

HB Compliance Conferences Webinar

February 26, 2016

The Revolution Will Be Worn on Your Wrist, Part 1 and 2

Kirk J. Nahra, Moderator

ABA Health Law Section's 17th Annual Conference on Emerging Issues in Healthcare Law

March 3, 2016 | San Diego, CA

Hack that 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

Cyber & Data Risk Insurance and Its Related Litigation Issues and Coverage Disputes

Laura A. Foggan, Speaker

ACI's 2016 Data Breach & Privacy Litigation and Enforcement Conference

March 17, 2016 | Philadelphia, PA

What's Next for Health Care Privacy?

Kirk J. Nahra, Speaker

Twenty-Fourth National HIPAA Summit

March 21-23, 2016 | Washington, DC

Enhancing Public Safety with Unmanned Aircraft

Anna Gomez, Moderator

IWCE International Wireless Communications Expo

March 24, 2016 | Las Vegas, NV

Privacy Bootcamp

Kirk J. Nahra, Speaker

IAPP Global Privacy Summit 2016

April 3, 2016 | Washington, DC

The Changing Face of Health Care Privacy

Kirk J. Nahra, Speaker

IAPP Global Privacy Summit 2016

April 6, 2016 | Washington, DC

Are You and Your Insurer Connecting on Cyber Risk?

Laura A. Foggan, Speaker

Northeast Corporate Counsel Forum 2016

April 21, 2016 | Atlantic City, NJ

Cybersecurity: Navigating a Terrain Fraught with Peril

Kirk J. Nahra, Speaker

International Franchise Association's 49th Annual Legal Symposium

May 16 & 17, 2016 | Washington, DC

Top New Privacy & Security Topics to Watch for in 2016

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association 2016 National Summit

May 18, 2016 | Orlando, FL

Contributing Authors

Jeremy J. Broggi	202.719.3747	jbroggi@wileyrein.com
Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Nova J. Daly	202.719.3282	ndaly@wileyrein.com
Laura A. Foggan	202.719.3382	lfoggan@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Umair Javed	202.719.7475	ujaved@wileyrein.com
Kathleen A. Kirby	202.719.3360	kkirby@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