Client Update
A Week of Hot News in Cybersecurity and Data Privacy

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Lawrence K. Cagney
lkcagney@debevoise.com

Jonathan F. Lewis
jflewis@debevoise.com

Ethan D. Roman
edroman@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

David A. Luigs
daluigs@debevoise.com

Naeha Prakash
nprakash@debevoise.com

FRANKFURT
Dr. Friedrich Popp
fpopp@debevoise.com

"Life moves pretty fast. If you don't stop and look around once in a while, you could miss it." Ferris Bueller's iconic advice always applies to the rapidly changing world of cybersecurity and data privacy, but rarely more so than last week. Here, we briefly report on a remarkable flurry of developments. Click on the links in this paragraph to jump to the update that interests you most, or simply read on to learn about: (1) the release of detailed information about the EU-U.S. Privacy Shield Framework; (2) the Consumer Financial Protection Bureau's first-ever enforcement action relating to data security; (3) the RSA Conference 2016 in San Francisco, always one of the year's leading events in this space; and (4) the U.S. Supreme Court decision in *Gobeille v. Liberty Mutual Insurance Company*, which addressed a state's ability to compel private companies to supply healthcare data.

EU-U.S. PRIVACY SHIELD FRAMEWORK

On February 29, the U.S. Department of Commerce and the European Commission made the full draft text of the EU-U.S. Privacy Shield Framework (the "Framework") available to the public. The Framework is intended to replace the Safe Harbor arrangement previously invalidated by the European Court of Justice ("CJEU") and to ensure that personal data can lawfully flow for commercial purposes from companies in the 28 EU Member States and the three European Economic Area members to U.S. organizations that self-certify compliance with the Privacy Shield requirements.

EU Individuals' Rights and Legal Remedies

The Framework provides that individuals in the EU will be able to bring complaints to participating organizations ("Participants"), which will have to respond to the individuals within 45 days. Participants also will have to provide, at no cost to the individual, an independent recourse mechanism through which complaints and disputes can be investigated and resolved; the mechanism may

be a panel established by European data protection authorities ("DPAs") or an EU- or U.S.-based alternative dispute resolution provider. If individuals instead opt to submit complaints to the DPAs, then the Department of Commerce will receive, review, and attempt to resolve the complaint, and respond to the DPAs within 90 days.

Individuals also will be able to pursue legal remedies through private actions in U.S. state courts, under the Judicial Redress Act signed by President Obama on February 24. Participants must agree to binding arbitration if an individual has raised a complaint to the Participant, made use of the Participant's independent recourse mechanism and raised the issue through the individual's DPA if those mechanisms have left a claim of a violation against the individual fully or partially unresolved.

Program Oversight and Cooperation with DPAs

The Department of Commerce has committed to administering and supervising the Framework, including but not limited to: (1) verifying information of Participants; (2) following up with former Participants to verify the treatment of personal information received during their participation; (3) searching for and addressing false claims of participation; (4) conducting periodic compliance reviews and assessments; and (5) cooperating with DPAs, which will entail establishing a liaison at the Department of Commerce, assisting DPAs seeking information on Participants or implementation of Framework requirements, and providing DPAs with material on the Framework to post on their websites in order to increase transparency for EU citizens and businesses.

The U.S. Federal Trade Commission ("FTC") has committed to cooperate with DPAs regarding (1) designating a point of contact at the agency for DPA referrals; (2) exchanging information with referring enforcement authorities; (3) working with DPAs on enforcement assistance; and (4) prioritizing referrals from DPAs, the Department of Commerce, privacy self-regulatory bodies and independent recourse mechanisms.

The Department of Commerce, FTC and other agencies will hold annual meetings with the EU Commission, interested DPAs, and representatives from the EU Article 29 Working Party, discussing current issues on the functioning, implementation, supervision and enforcement of the Framework.

Requirements for Participants

Participants in the Framework must be subject to the jurisdiction of the FTC, the Department of Commerce or another statutory body able to ensure compliance

with the Framework. The text leaves open the possibility of the EU recognizing such statutory bodies in future annexes. A Participant will have to include in its privacy policy a declaration committing to compliance with the Privacy Shield Principles, the set of rules detailing the organization's data protection obligations, making the commitment enforceable under Section 5 of the Federal Trade Commission Act.

If the privacy policy is online, it will have to include a link to the Department of Commerce's Privacy Shield website and a link to the independent recourse mechanisms available to address individual complaints. Participants also will have to inform individuals of their rights regarding their personal data and which enforcement authority has jurisdiction over compliance with the Framework. The Framework limits the amount of personal information collected by Participants to only the information relevant for the purposes of processing.

Participants will be required to take steps to ensure accountability for data transferred to third parties, including (1) limiting and specifying the purposes for which third parties may use personal information, including verifying that the third party will provide the same level of protection as the Privacy Shield Principles; and (2) taking reasonable and appropriate steps to ensure the third party's access to and use of personal information is limited, authorized and documented.

Participants must cooperate with the Department of Commerce regarding inquiries relating to the Framework, ensure transparency of compliance or assessment reports submitted to the FTC and even if withdrawing from the Framework, annually certify compliance with Privacy Shield Principles for information received under the Framework.

Limitations on National Security and Law Enforcement Access to Data

As part of the Framework, the U.S. intelligence community and U.S. Department of Justice have provided to the EU information on the safeguards and limitations that apply to their operations. The Framework also establishes a channel for EU individuals to raise questions regarding signals intelligence practices. The U.S. Department of State has committed to establish a point of contact for these types of inquiries, and the United States has committed to responding to appropriate requests regarding these matters.

What Next for the Framework?

The draft text is now subject to review by the EU Article 29 Working Party, by a Committee composed of EU Member States representatives and the European Data Protection Supervisor. It remains possible that the Working Party could raise objections. Although technically, this would not hinder the Commission from adopting the Framework, the support of both the Working Party and the independent national DPAs will ultimately impact the efficiency of this data transfer mechanism. Currently, it is expected that the Framework will take legally binding effect in a few months, once the United States has made the necessary preparations. Of course, once the Privacy Shield is adopted, new challenges could be brought in the CJEU.

What Should Companies Do Right Now?

While the substantive provisions of the Framework could still change, last week's release provides a clear roadmap of specific tasks for companies that want to start preparing for compliance. Key tasks would include assessing your privacy policies in light of the Privacy Shield Principles and determining what provisions need to be added and where; assessing options for the creation of the independent recourse mechanism for EU individual complaints; and assessing your contracts and relationships with third parties who handle data on your behalf. Steps like these should enable you to be ready to operate under the Framework more quickly once it is approved.

CFPB'S FIRST-EVER DATA SECURITY CASE

On March 2, the Consumer Financial Protection Bureau ("CFPB" or "Bureau") took action against Dwolla, an online payment platform, for deceiving its customers about its data security practices and its online payment system. This is the first data security enforcement action by the Bureau, through the use of its statutory authority to punish unfair, deceptive and abusive acts or practices ("UDAAP"). CFPB has now joined a long list of regulators, ranging from (for example) the SEC to the FTC to the FCC to the attorneys general of the 50 states, that are looking to make high-impact cyber cases.

Dwolla collects personal information including the customer's name, address, date of birth, telephone number, Social Security number, and bank account and routing numbers. Dwolla told customers it had set "a new precedent for the payments industry," providing "safe" and "secure" transactions and protecting personal information through data security practices that would "exceed" or "surpass" industry standards. Dwolla asserted, in particular, that it encrypted sensitive personal information and that its mobile applications were safe and secure.

CFPB found that Dwolla's data security practices in fact fell far short of its claims, and therefore took enforcement action even though Dwolla had not suffered a data breach. Specifically, the CFPB found, among other issues, that Dwolla failed to employ reasonable and appropriate measures to protect customer data; encrypted only some of the personal information in its systems; and released mobile applications before testing whether they were secure.

The Bureau thus ordered Dwolla to stop deceiving its customers about the security of its data, enact and train employees on new data security measures and policies, train employees how to protect customer data, fix any security weaknesses in its web and mobile applications and securely store and transmit customer data going forward. The CFPB also ordered Dwolla to pay a $100,000 civil monetary penalty.

What Should Companies Do Right Now?

To reduce UDAAP risk, modesty may be the new order of the day in how a company should describe its cybersecurity practices to customers. Companies might also consider regularly cross-checking the statements about cybersecurity in their privacy policies, terms of service, and other communications to consumers against the level of security actually being provided. In conducting such a cross-check, companies should keep in mind the theory used in the Dwolla case: a company can be in violation of the law merely for having a mismatch between your public statements and your private practices – even without a data breach or consumer harm. The Dwolla case also shows that regulators are increasingly confident in concluding that specific technical gaps, such as incompleteness of encryption, can drive a finding of legal violation.

RSA CONFERENCE 2016

RSA Conference 2016 took place in San Francisco, CA, from February 29 through March 4. The annual conference, which began in 1991 as a forum for cryptographers to share knowledge and advancements in the area of Internet security, has grown into a major opportunity for information security professionals around the world to discuss the most pressing issues in the field.

Joining data security professionals and tech company CEOs on the speakers list were Admiral Michael R. Rogers, Commander of the U.S. Cyber Command and Director of the National Security Agency, Secretary of Defense Ashton B. Carter, and Attorney General Loretta Lynch. The Attorney General noted that online adversaries are posing significant threats to national security and highlighted the work that the Department of Justice does in fighting cybercrime as "a defense of American ideals."

Other speakers focused on cybersecurity risk reduction, data loss prevention and encryption techniques. On these and other topics, they underscored that cybersecurity issues require inter-governmental and inter-agency coordination and public-private partnership. The panel "Beyond Encryption: Why We Can't Come Together on Security and Privacy – and the Catastrophes That Await if We Don't" featured former Secretary of Homeland Security, Michael Chertoff and former Director of National Intelligence, Mike McConnell, among others. They discussed the challenges of balancing national security and individual privacy, the need to do so, and the need for government to provide the private sector with the technical tools—as well as the laws—that it needs to be a good partner.

Details on these and other RSA panels, including a keynote by none other than Sean Penn, are available on the excellent conference blog. The topics at RSA Conference 2016 are sure to be on the forefront of public and private actions over the next year. Companies will benefit from keeping up to date on public sector activity, anticipating new laws and regulations on cybersecurity and data privacy, and having a plan in place to react to the rapidly changing legal and regulatory landscape.

Concurrent with the RSA conference was the unveiling of the latest Verizon Data Breach Digest Report. The report is a rich compendium of information about specific breach incidents and larger trends, and well worth perusing.

The report documents, for example, an incident suffered by a global shipping company that had experienced a series of hit-and-run attacks by pirates. The pirates appeared to have specific knowledge of the contents of shipping crates; instead of seeking a ransom, the pirates would board a vessel, locate by bar code specific sought-after crates containing high-value cargo, steal the contents and depart the vessel. An examination of network traffic revealed that the computer systems of the shipping company itself had been compromised. This gives a new meaning to the term "piracy," and offers a sharp reminder of the many kinds of disruption that hackers can cause throughout the global economy.

GOBEILLE V. LIBERTY MUTUAL INSURANCE COMPANY

On March 1, the U.S. Supreme Court released its opinion in *Gobeille v. Liberty Mutual Insurance Company*. In a 6-2 decision written by Justice Kennedy, the Court held that a Vermont statute requiring health insurers to provide data about the healthcare services provided to Vermont citizens was preempted by the Employee Retirement Income Security Act of 1974 ("ERISA"). *Gobeille* is not a case about personal information or data privacy *per se*; the data that Vermont had required from insurers was aggregated and anonymized. The case still bears a

look from privacy professionals for the light it shines on how companies and governments may handle information, especially healthcare information, going forward.

The case arose when Vermont tried to coerce Liberty Mutual's health plan and Blue Cross Blue Shield, the plan's third-party administrator, to turn over voluminous data regarding plan participants' claims, cost and utilization. Because Liberty Mutual was exempt from the statute (because the plan did not cover enough Vermont residents), Vermont focused its demands on Blue Cross Blue Shield. Liberty Mutual, fearing that participants could sue Liberty Mutual under ERISA if the data were released, directed Blue Cross Blue Shield not to comply with the law.

In keeping with the Court's historically broad interpretation of ERISA preemption, the Court held that ERISA preempts the Vermont law that imposed additional reporting requirements on health plans and related plan administrators. Justice Kennedy's opinion noted that ERISA has extensive reporting, disclosure and recordkeeping requirements, including an annual report filed with the Secretary of Labor which includes listing assets and liabilities for the previous year, as well as receipts and disbursements of funds. The Court held that these reporting requirements "are central to, and an essential part of plan administration contemplated by ERISA."

By adding to these requirements, Vermont's statute had the potential to "create wasteful administrative costs and threaten to subject plans to wide-ranging liability." Decisions on whether to require data reporting, the majority held, therefore appropriately belong to federal, not state, authorities. Numerous other states have laws similar to Vermont's, which presumably fail after *Gobeille*.

In a concurring opinion, Justice Breyer noted that although Vermont's law was preempted by ERISA, the Secretary of Labor could implement reporting requirements that would allow states to collect data in a similar manner to Vermont's statute, or could delegate to states the authority to collect data and provide the data to the federal government.

As relating to data privacy, this case serves as a reminder for some key principles: (1) an employer's third-party vendors (here, Blue Cross Blue Shield) may have reams of sensitive employee data; (2) third-party vendors may themselves be subject to disclosure obligations; (3) a vendor's compliance with disclosure requirements may subject the employer to legal risk; and (4) different regulators may plow ahead with their regulatory mission without due regard for other disclosure regimes, thus creating the risk of conflicting legal obligations (as well

as employer-vendor conflict). In addition, greater effort to see around these corners may be warranted when dealing with pension plan and health plan data in light of ERISA's high fiduciary standards (as well as risk presented by the number of current and former employees, all of whom are potential plaintiffs).

Companies should also be aware of the possibility of future federal government rulemaking requiring them to share customer data with state or federal regulators, particularly in light of Justice Breyer's call for such a rule. And while *Gobeille* is industry- and ERISA-specific, the possibility of federal-state tension over who can compel various kinds of data collection and reporting is not necessarily so limited. Observers will be watching to see how it might resurface in other contexts.

* * *

Consistent with Ferris's advice, we will continue to watch these and other issues. Please do not hesitate to contact us with any questions.