Cyber Update
28 January 2019
By Michael Kans

EDPB Details Its Misgivings About Privacy Shield

Last week, the European Union's (EU) data protection authorities (DPA) adopted the European Data Protection Board (EDPB) "EU-U.S. Privacy Shield - Second Annual Joint Review," which noted some progress by the United States (U.S.) in implementing the EU-U.S. Privacy Shield. However, the EU's DPAs and EDPB took issue with a number of shortcomings in U.S. implementation, many of which have been noted in previous analyses of U.S. efforts to ensure that U.S. companies that agree to the Privacy Shield's principles regarding the processing the personal data of EU citizens transferred out of the EU. Notably, the EDPB found problems with the assurances provided by the U.S. government regarding the collection and use of personal data by national security and law enforcement agencies. The EDPB also found problems with how the Department of Commerce and Federal Trade Commission are enforcing the Privacy Shield in the U.S. against commercial entities.

The Privacy Shield "provide[s] organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries." The agreement became effective in August 2016 and replaced the International Safe Harbor Privacy Principles that the European Court of Justice struck down in October 2015.

The EDPB "welcome[d] the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions, as well as the efforts made by the U.S Government by publishing a number of important documents and the appointment of a new Chair as well as of two new members of the Privacy and Civil Liberties Oversight Board (PCLOB), meaning that the PCLOB has reached the required quorum for its functioning." The EDPB stated it "still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities."

The EDPB stated that "[t]he absence of substantial checks remains a concern…[and] [o]ther areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR Data and processors, as well as the

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans

recertification process." The EDPB noted "the remaining issues with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016."

The EDPB encouraged the PCOLB "to issue further reports, including on Presidential Policy Directive 28 (PPD-28) to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, on Section 702 [of the Foreign Intelligence Surveillance Act (FISA)], and Executive Order 12333." The EDPB noted it is "still awaiting the appointment of a permanent independent Ombudsperson…[and] [g]iven the elements provided, the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non- compliance, and it can thus not state that the Ombudsperson can be considered an 'effective remedy before a tribunal.'"

While the EU has not threatened to suspend the Privacy Shield, in December 2018, the European Commission set a deadline of February 28, 2019 by which the U.S. must have an Ombudsman nominated but not confirmed. The European Commission stated that "If this does not take place by that date, the Commission will then consider taking appropriate measures, in accordance with the General Data Protection Regulation." Also, there are legal challenges against Privacy Shield that could bring about significant changes to the trans-Atlantic deal or strike it down all together.

More Committee Assignments Announced

The House Armed Services Committee announced that Representative James Langevin (D-RI) will chair the Intelligence, Emerging Threats, and Capabilities Subcommittee and Representative Elise Stefanik (R-NY) will be the ranking member. The House Judiciary Committee named Representative Hank Johnson (D-GA) as the chair of the Courts, Intellectual Property, and the Internet Subcommittee, and Representative Martha Roby (R-AL) will be the ranking member.

However, while the House Oversight and Government Reform Committee has not named subcommittee chairs and ranking members, word was leaked this week that the Information Technology Subcommittee will be eliminated and its jurisdiction likely transferred to the Government Operations Subcommittee. One reason for this move may be that Representative Robin Kelly's (D-IL) assignment to the House Energy and Commerce Committee removed the Member posed to fight for the continued existence of the subcommittee as she stood to hold the gavel in this Congress. Additionally, former chair Will Hurd (R-TX) won a seat on the House Appropriations Committee, and it is unclear whether he will have to relinquish his seat on the Oversight and Government Reform Committee.

However, Speaker Nancy Pelosi (D-CA) announced the new Democratic Members of the House Oversight and Government Reform Committee, including those with other committee jurisdictions that intersect on cybersecurity and data security and some high-profile freshmen:

- Congressman Mark DeSaulnier of California
- Congressman Jimmy Gomez of California
- Congresswoman Katie Hill of California
- Congresswoman Robin Kelly of Illinois
- Congressman Ro Khanna of California
- Congresswoman Brenda Lawrence of Michigan
- Congresswoman Alexandria Ocasio-Cortez of New York
- Congresswoman Stacey Plaskett of U.S. Virgin Islands
- Congresswoman Ayanna Pressley of Massachusetts
- Congressman Harley Rouda of California
- Congressman John Sarbanes of Maryland
- Congresswoman Jackie Speier of California
- Congresswoman Rashida Tlaib of Michigan
- Congresswoman Debbie Wasserman Schultz of Florida
- Congressman Peter Welch of Vermont

The Senate Commerce, Science, and Transportation Committee announced their subcommittee rosters, including the ranking members. Here are the chairs and ranking members of the subcommittees with jurisdiction over data security, cybersecurity, and privacy issues:

- Communications, Technology, Innovation and the Internet
  - Chairman John Thune (R-SD) – Chairman
  - Ranking Member Brian Schatz (D-HI)
- Manufacturing, Trade, and Consumer Protection
  - Chairman Jerry Moran (R-KS)
  - Ranking Member Richard Blumenthal (D-CT)
- Security
  - Chairman Dan Sullivan (R-AK)
  - Ranking Member Edward J. Markey (D-MA)

New Cyber Agency Directs Agencies To Secure Email and Domains

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 19-01, "Mitigate Domain Name System (DNS) Infrastructure Tampering," directing federal agencies to take steps to remedy weaknesses that hackers based in Iran may be exploiting. CISA asserted that "attackers have redirected and intercepted web and mail traffic, and could do so for other networked services." CISA makes clear that this directive does "not apply to statutorily- defined "national security systems" nor to systems operated by the

Department of Defense or the Intelligence Community." However, it does include "such systems used or operated by another entity on behalf of an agency," meaning it covers many if not most information technology (IT) contractors and subcontractors.

CISA's emergency directive follows media reports and publicly available analyses by security firms (FireEye and Cisco Talos Intelligence) that point to Iran as the source of widespread DNS hacking throughout the Middle East, North Africa, Europe, and North America. In early January, DHS' National Cybersecurity and Communications Integration Center (NCCIC) released an alert on these hacking activities. CISA stated that it "is aware of multiple executive branch agency domains that were impacted by the tampering campaign and has notified the agencies that maintain them."

CISA explained that "[u]sing the following techniques, attackers have redirected and intercepted web and mail traffic, and could do so for other networked services.

1. The attacker begins by compromising user credentials, or obtaining them through alternate means, of an account that can make changes to DNS records.
2. Next, the attacker alters DNS records, like Address (A), Mail Exchanger (MX), or Name Server (NS) records, replacing the legitimate address of a service with an address the attacker controls. This enables them to direct user traffic to their own infrastructure for manipulation or inspection before passing it on to the legitimate service, should they choose. This creates a risk that persists beyond the period of traffic redirection.
3. Because the attacker can set DNS record values, they can also obtain valid encryption certificates for an organization's domain names. This allows the redirected traffic to be decrypted, exposing any user-submitted data. Since the certificate is valid for the domain, end users receive no error warnings.

CISA stated that:

> To address the significant and imminent risks to agency information and information systems presented by this activity, this emergency directive requires the following near-term actions to mitigate risks from undiscovered tampering, enable agencies to prevent illegitimate DNS activity for their domains, and detect unauthorized certificates.

CISA detailed the "[r]equired [a]ctions" civilian agencies must take:

- Action One: Audit DNS Records
- Action Two: Change DNS Account Passwords
- Action Three: Add Multi-Factor Authentication to DNS Accounts
- Action Four: Monitor Certificate Transparency Logs

CISA is requiring that these actions be completed by February 5, will follow up with those agencies that "have not completed required actions," and will submit a report to DHS and the Office of Management and Budget (OMB) by February 8 "identifying agency status and outstanding issues."

Vulnerabilities Disclosure and Bug Bounty Bill Passes

Last week, the House passed the "Hack Your State Department Act" (H.R. 328) by a 377-3 vote. This bill would require that the Department of State "design and establish a Vulnerability Disclosure Process (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State." This bill tracks closely with provisions in the "Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act" (P.L. 115-390), which tasked the Department of Homeland Security with executing both missions.

Leaders On House Committee Reintroduce Bill To Increase State Department Focus on Cybersecurity

The new Chairman and Ranking Member of the House Foreign Affairs Committee reintroduced a bill that would require the Department of State to reprioritize international diplomacy on cybersecurity. Representatives Eliot Engel (D-NY) and Michael McCaul (R-TX) introduced the "Cyber Diplomacy Act of 2019" (H.R. 739), legislation very similar to a bill the House passed by voice vote in the last Congress. The bill declares it "is the policy of the United States to work internationally to promote an open, inter-operable, reliable, unfettered, and secure Internet governed by the multi-stakeholder model." In their press release, Engel and McCaul explained the bill does the following:

- Establishes a high-level Ambassador for Cyberspace to lead the State Department's cyber diplomacy efforts and directs the U.S. Ambassador to the United Nations to advance international cyberspace policy;
- Creates a U.S. international cyber policy that advances democratic principles and rejects attempts by Russia and China to extort more control and censorship over the internet;
- Specifies key objectives for implementing the strategy, including securing commitments on responsible state behavior, and requires regular updates to the strategy;
- Promotes working with foreign governments to support the United States international cyberspace policy and establishes a congressional notification process for preexisting and future arrangements; and
- Requires the State Department's annual country report on human rights to include assessments related to internet freedoms.

In early 2018, former Secretary of State Rex Tillerson had eliminated the Office of the Cybersecurity Coordinator and rolled this position's responsibilities into the Bureau of Economic Affairs' Office of International Communications and Information Policy. This move was greeted by displeasure from both sides of the aisle and after pressure from Congressional stakeholders did not work, legislation was drafted. Former House Foreign Affairs Committee Chairman Ed Royce (R-CA) and Engel had introduced the "Cyber Diplomacy Act of 2018" (H.R. 3376 (115)) that passed the House by voice vote and was sent to the Senate floor by the Senate Foreign Relations Committee where it eventually died.

Senate Democrats Call on Federal Agencies To Investigate Telecoms Sharing of Geolocation Data

Last week, 15 Senate Democrats called on the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) "to investigate how wireless carriers allowed third parties – including data brokers and bounty hunters – to track Americans' cell phones without consent" according to their press release. In their letter, they urged the FCC and FTC "to conduct broad investigations, as appropriate, into the business partnerships between wireless carriers and location aggregators, including resellers and all downstream buyers of location data." This letter was prompted by a *Motherboard* article that alleged "T-Mobile, Sprint, and AT&T are selling access to their customers' location data" and follows letters sent by House Energy and Commerce Democrats and Republicans. Nonetheless, both the FCC and FTC have been shuttered due to the ongoing lapse in funding affecting a number of federal agencies and may not be able to respond as fully as lawmakers would like.

The signatories include the Senate Minority Leader, two announced candidates for president and three more rumored candidates:

- Ron Wyden (D-OR)
- Chuck Schumer (D-NY)
- Ed Markey (D-MA)
- Richard Blumenthal (D-CT)
- Kamala Harris (D-CA)
- Patrick Leahy (D-VT)
- Jeff Merkley (D-OR)
- Ben Cardin (D-MD)
- Sheldon Whitehouse (D-RI)
- Amy Klobuchar (D-MN)
- Kirsten Gillibrand (D-NY)
- Cory Booker (D-NJ)
- Jack Reed (D-RI)

- Tina Smith (D-MN)
- Bernie Sanders (I-VT)

Earlier this month, House Energy and Commerce Committee Chairman Frank Pallone Jr. (D-NJ) sent a letter to the FCC asking for a briefing to explain why the FCC "has yet to end wireless carriers' unauthorized disclosure of consumers' real-time location data and what actions the FCC has taken to address this issue to date." Pallone asserted that these issues were addressed in the rewrite of telecommunications law in 1996, but that the FCC has "dragged its feet in protecting consumers."

A week later, Republican leadership on the House Energy and Commerce Committee sent letters to Zumingo, Microbilt, T-Mobile, AT&T, Sprint, and Verizon, "requesting information…about the sale and misuse of cell phone geolocation data" according to the their press release. Republicans claimed that their "letters seek to increase transparency surrounding how U.S. wireless carriers and third parties are accessing, transferring, storing, and securing customer location information." They also asserted that "[t]he letters also build off letters the committee sent last year to location aggregation companies LocationSmart, Securus Technologies, and 3C Interactive." The letters pose a number of questions to these companies regarding their privacy practices and whether consumers have affirmatively opted into the regime under which their location information is shared or sold with third parties. Republicans have also requested that these companies brief committee staff by January 30, 2019.

New National Intelligence Strategy Stresses Threats Posed By Cyber and Information Operations

Last week, the Director of National Intelligence (DNI) released the "National Intelligence Strategy" (NIS), and DNI Dan Coats warned that adversarial nation states and others are using current technologies in ways that posed threats to the U.S. and that new technologies will likely lead to additional ways for the U.S. to be challenged. The DNI explained that one of the NIS' seven mission objectives is "Cyber Threat Intelligence," which is "[d]etect[ing] and understand[ing] cyber threats from state and non-state actors engaged in malicious cyber activity to inform and enable national security decisionmaking, cybersecurity, and the full range of response activities."

The DNI explained

> Despite growing awareness of cyber threats and improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come. Our adversaries are becoming more adept at using cyberspace capabilities to threaten our interests and advance their own strategic and

economic objectives. Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices. The Intelligence Community (IC) must continue to grow its intelligence capabilities to meet these evolving cyber threats as a part of a comprehensive cyber posture positioning the Nation for strategic and tactical response.

The IC pledged to:

- Increase our awareness and understanding of adversaries' use of cyber operations—including leadership plans, intentions, capabilities, and operations—to inform decisions and enable action.
- Expand tailored production and appropriate dissemination and release of actionable cyber threat intelligence to support the defense of vital information networks and critical infrastructure.
- Expand our ability to enable diplomatic, information, military, economic, financial, intelligence, and law enforcement plans and operations to deter and counter malicious cyber actors and activities.