March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Google Receives Record GDPR Fine

Marking the first major penalty against a U.S. tech company under the General Data Protection Regulation (GDPR), the French data-protection authority, CNIL, has fined Google a record $57 million. Google's violations stemmed from a lack of transparency regarding how it uses consumers' personal information and from a failure to obtain sufficiently informed consent to use that information to personalize ads. CNIL's investigation began on May 25, 2018—the day the GDPR took effect—in response to concerns raised by two groups of privacy activists. While the fine represents a fraction of the maximum possible penalty of $4.7 billion, the move should put other U.S. tech companies on high alert that European regulators will apply tough scrutiny under the sweeping data-protection law.

Read CNIL's statement and *The Washington Post* article >>

Privacy Activist Files Bevy of GDPR Complaints

Austrian attorney and privacy activist Max Schrems has filed several GDPR complaints with the Austrian data-protection authority, naming Amazon, Netflix, YouTube and other major technology companies. The complaints allege that the companies failed to fully comply with data-subject information requests. Schrems, who leads the non-profit noyb (none of your business), has demonstrated that privacy groups will continually test companies' compliance with the GDPR; he filed complaints in 2018 against Google, Facebook, Instagram and WhatsApp.

SUBSCRIBE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

Read the *Reuters* article >>

Stepping into the Federal Void, States Introduce Comprehensive Privacy Laws and Other Measures

Following on the heels of the California Consumer Privacy Act (CCPA), legislation introduced in the New Mexico and Washington state legislatures would greatly expand consumer-privacy protections in those states. The New Mexico bill, SB 176, largely incorporates the same provisions as the CCPA, while the Washington bill, SB 5376, incorporates concepts from the GDPR. One major difference is that the New Mexico bill provides for a private right of action while the Washington bill would be enforceable only by the state attorney general. The laws would take effect on July 1, 2020, and December 31, 2020, respectively.

Legislators in Massachusetts have also introduced a CCPA-style privacy law that would take effect January 1, 2023. The law provides for a private right of action, and, significantly, explicitly states that a mere technical violation would provide a plaintiff standing to sue, a heavily litigated issue under the Illinois biometric privacy law.

Other states are also looking to enact stricter privacy provisions. Legislators in New York have proposed several measures, including a private right of action for data-breach victims and a prohibition on the use of biometric data for marketing and advertising purposes. A Virginia bill would allow minors to request removal of information and impose additional restrictions on marketing, advertising and data sharing. A law introduced in Utah would restrict government agencies' ability to obtain personal information, and North Dakota is considering a bill that would require affirmative consent before an entity discloses personal information.

Read *The Information* article >>

Yahoo Settles Derivative Suits Over Data Breaches, But Data-Breach Settlement Rejected

After a $35 million settlement with the Securities and Exchange Commission in 2018 for failing to timely disclose a 2014 breach affecting more than 500 million users, Yahoo (now Altaba) has settled three shareholder derivative lawsuits related to a series of cyberattacks from 2013 to 2016. The plaintiff shareholders alleged

Colman McCarthy
Associate
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate
813.202.7151
kpaine@shb.com

Alyse Zadalis
Associate
816.559.2323
azadalis@shb.com

that Yahoo's directors and officers breached their fiduciary duties with their handling of customer information in relation to those cyberattacks. The $29 million settlement marks the first time shareholders have been awarded monetary damages in a breach-related derivative lawsuit.

Yahoo's attempt to settle a related consumer class-action lawsuit, however, was rejected by Judge Koh of the Northern District of California. Judge Koh rejected the proposed $50 million settlement on multiple grounds, finding the amount allocated to victims too vague, the attorneys' fees too high and a shortage of required enhanced security measures.

Read *The New York Times* article and the *Courthouse News* article >>

North Carolina to Propose Amendments to Data-Breach Law

After recent increases in the number of North Carolina residents affected by data breaches, State Rep. Jason Saine, accompanied by State Attorney General Josh Stein, announced that he would be proposing amendments to the state's data-breach-notification law. While the legislation is still being drafted, its provisions will reportedly include a new 15-day deadline to provide notification of a breach, a requirement to maintain reasonable security procedures and practices, and a mandatory five years of free credit monitoring for victims of a breach.

Read the *Carolina Journal* article >>

EU and Japan Agree to Allow Data Flows

Building on their July 2018 agreement to recognize each other's data-protection systems as adequate, the European Commission and Japan have formally adopted that adequacy decision. The decision takes effect immediately, allowing freer flow of data between Japan and the European Union. It will also complement the EU-Japan Economic Partnership Agreement, which enters into force in February 2019.

Read the EU press release >>

Shutdown Affected Federal Government's Privacy and Cybersecurity Work

The federal government's partial shutdown of December 2018–January 2019 has complicated the work of various agencies with regards to privacy and cybersecurity matters. The Department of Homeland Security and the Federal Trade Commission (FTC) furloughed staff who focus on privacy issues, while other agency employees were restricted in the amount of time they could spend on privacy matters, resulting in delays to investigations and risk assessments. The Federal Bureau of Investigation also saw cybersecurity probes hamstrung by a lack of funds, subpoena delays and an inability to collaborate with other government agencies.

Read the IAPP's article and the *Bank Info Security* article >>

Facebook May Receive Record FTC Fine

FTC may impose a record-setting fine on Facebook following an alleged violation of a 2011 consent decree requiring the company to protect its users' personal data. The fine is reportedly projected to be larger than the $22.5 million fine Google received in 2012, which at the time set a record for the largest penalty imposed for violations related to improving privacy practices.

Read *The Washington Post* article >>

The Push for National Privacy Legislation Gains Steam

Calls for national privacy legislation continue to arise, due in part to the enforcement of the GDPR, the passage of the California Consumer Privacy Act and various privacy-related incidents at major companies such as Facebook and Marriott Hotels. Multiple constituencies are forming to press their visions to Congress. Among the competing proposals are bills introduced by Democratic and Republican senators, a group of privacy organizations' proposal for a new federal agency and a privacy framework of baseline protections formulated by the Information Technology and Innovation Foundation, a think tank backed by major tech companies.

Read the *Associated Press* article >>

Huawei Indicted for Alleged Theft of Trade Secrets, Wire Fraud and Obstruction of Justice

An unsealed indictment has revealed that the Department of Justice (DOJ) has charged Chinese device-maker Huawei with stealing trade secrets from T-Mobile. According to the indictment, Huawei employees violated confidentiality and non-disclosure agreements and stole equipment related to a T-Mobile phone-testing robot. Huawei also allegedly offered bonuses to employees based on the value of information they stole from other companies.

Read the DOJ statement >>

U.K.'s ICO Releases Guidance on Brexit

While the terms on which the United Kingdom will exit the EU are subject to ongoing debate, the Information Commissioner's Office has released guidance on personal-data flows to the European Economic Area after Brexit is completed. The ICO published the guidance, along with associated tools, to help organizations prepare for a future in which data flows are not provided for in the United Kingdom's withdrawal from the EU. The ICO's primary advice is to continue complying with the GDPR, as the United Kingdom plans to incorporate the GDPR into U.K. law after Brexit.

Read ICO's guidance >>