September 2019

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

California Adds Biometric Restrictions to Data-Breach Law, Potentially Creating a *De Facto* Biometric Privacy Law

Subject to the governor's signature, California's breach-notification law will gain additional requirements related to biometric information due to the passage of AB 1130. The bill adds "unique biometric data" to the definition of personal information where that data is generated from measurements or analysis of body characteristics for authentication purposes. Going forward, notices for breaches involving biometric data must include instructions on how to notify third parties to no longer rely on the compromised data for authentication purposes.

TAKEAWAY

This change, in combination with the California Consumer Privacy Act's (CCPA's) private right of action, may create a *de facto* biometric privacy law in California that allows for a private right of action where there is unauthorized disclosure of biometric information (e.g., a merchant/employer sharing biometric information with a third-party provider) and a lack of policies and procedures governing biometric information.

Researcher Exploits GDPR Request Procedures

A security expert working to gauge General Data Protection Regulation (GDPR) compliance reportedly used the law's request mechanism to gain access to data about another individual. Pretending to be his fiancée, the expert contacted 83 companies of various sizes and found that mid-sized companies that knew of the GDPR but did not have proper data-breach protocols in place

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

fell victim to the attack more than large or small companies. Some failures included (i) releasing criminal history, (ii) allowing access to a gaming account without proper verification and (iii) providing a list of breached usernames and passwords that worked on other websites the expert's fiancée uses.

TAKEAWAY

Companies should scrutinize information provided by an individual during the data-subject-request process and not simply take that information at face value. Shook privacy attorneys Al Saikali and Kate Paine provide detailed guidance on the GDPR verification process in an article for *Financier Worldwide*.

Update: Federal Court Upholds $925 Million TCPA Verdict against ViSalus

As noted in our May alert, an Oregon jury awarded $925 million in damages after determining ViSalus violated the Telephone Consumer Protection Act (TCPA) with 1.85 million improper robocalls to individuals. ViSalus attempted to mitigate the verdict post-trial by seeking class decertification, basing its argument on a retroactive waiver it received from the Federal Communications Commission (FCC) related to many of the calls underlying the verdict. The district court was not persuaded, rejecting ViSalus's request due to the company's failure to plead consent as an affirmative defense and request the court stay the case pending FCC's decision.

TAKEAWAY

The potential for substantial damages under the TCPA make it imperative to assert and pursue all affirmative defenses in a timely manner.

FTC Settles with Five Companies Falsely Claiming Privacy-Framework Compliance

The Federal Trade Commission (FTC) settled separate actions against five companies after they falsely promoted compliance with the EU-U.S. Privacy Shield framework. In reality, the five companies either failed to finish the certification process or allowed their certification to lapse. One of the companies also misrepresented its compliance under the Swiss-U.S. Privacy Framework. The settlement includes directives that all five companies refrain from misrepresenting their levels of compliance under any privacy or data-security program. No monetary penalties were issued.

TAKEAWAY

Colman McCarthy
Associate
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate
813.202.7151
kpaine@shb.com

Ben Patton
Associate
206.344.7625
bpatton@shb.com

Lischen Reeves
Associate
816.559.2056
lreeves@shb.com

Privacy Shield certification is burdensome but worthwhile. Businesses should take care when using Privacy Shield as a marketing strategy to ensure statements about compliance are accurate.

IAB Introduces Transparency and Consent Framework Plan 2.0

The Interactive Advertising Bureau (IAB) Europe has announced the Transparency and Consent Framework (TCF) 2.0, which provides GDPR compliance guidance to digital advertising companies. The new framework gives consumers the ability to object to the processing of any personal data and increased control over vendor usage of data processing features such as precise geolocation. Entities that publish consumer data can now restrict the reasons vendors may cite to process consumer data.

TAKEAWAY

Digital advertising is a complex field with many potential gray areas for compliance with privacy laws, and TCF 2.0 provides welcome guidance.

ISO Adds New Privacy Standard

The International Standards Organization (ISO) published ISO/IEC 27701, a privacy-centric extension to the commonly adopted security standard ISO/IEC 27001. The new standard aims to help all types and sizes of companies implement, maintain and continually improve a privacy-specific information-security-management system. While the new standard is meant to be jurisdiction-agnostic, use with GDPR compliance is clearly intended, with a section on GDPR mapping and CNIL contributions to the formation of the standard.

TAKEAWAY

Further signaling the importance of privacy, the ISO has added its authoritative voice to a long list of privacy standards.

FTC and New York AG Settle Kids' Privacy Case in Largest COPPA Settlement to Date

FTC and the New York attorney general's office have settled an action against Google and YouTube alleging that, in violation of the Children's Online Privacy Protection Act (COPPA), the companies failed to obtain the necessary parental/guardian consent before using cookies attached to the websites. The

settlement terms include $134 million to FTC, $36 million to New York, a requirement that both companies develop systems that allow content targeted at children to be flagged for COPPA compliance, and a requirement that YouTube's employees receive training on COPPA compliance.

TAKEAWAY
Businesses should not ignore the consequences of cookie usage, particularly where children are involved.

European Court Permits Police Use of Biometric Software

Following a request by human rights advocacy group Liberty to review the South Wales Police's (SWP's) use of software that scans and tracks biometric facial features, the Welsh high court has held that the use complies with data privacy laws. The group alleged the software, AFR Locate, violated the privacy rights of as many as 500,000 people during the 50 times it has been used. SWP uses the software to track and locate people involved in criminal activity, and it publicly announces when the software will be activated. Although the court agreed that SWP was processing personal data, it found the use of the software to be in compliance with data privacy laws, including the Data Protection Act 2018 and the Human Rights Act. The court's reasoning relied on evidence that the software was used only at a specific time and for a specific and limited purpose.

TAKEAWAY
Though the decision allows governmental use of facial-recognition technology, it recognized the potential for abuse and emphasized the constrained nature of the use. The ruling may provide a roadmap for future decisions in light of the likely inevitability of further such use.

Florida State Senator to Reintroduce Biometric Privacy Law

Florida Sen. Gary Farmer has signaled that he will reintroduce his biometric-privacy bill in the next legislative session. The bill, which previously died in committee, parroted the Illinois Biometric Information Privacy Act (BIPA), including BIPA's private right of action for "aggrieved" individuals. Critics are concerned the law will subject businesses to legal liability. The senator's office is interested in negating these views by welcoming the input of Florida business owners. Other states, including New York, Michigan and Alaska, are also considering passing biometric-privacy legislation.

TAKEAWAY

Given the repeated attempts to pass this legislation, companies conducting business in Florida should proactively review their use of biometric information. Nevertheless, given the political composition of the Florida Legislature, passage of this law anytime soon is unlikely.

SHOOK PRIVACY SPOTLIGHT

Benjamin Patton

With an extensive background in computer science and vast knowledge of technology relating to data security, Ben Patton is a critical member of Shook's Privacy and Data Security team. As a former software developer and security analyst, Ben helped create company-wide security awareness policies for developers at a major IT company and served as a consultant on internal security threats. Ben's substantial technical knowledge allows him to assess clients' cybersecurity issues and offer practical advice even as technology and data privacy law evolve. Ben has been involved in numerous incident response matters and worked closely with forensic firms to help mitigate and respond to data breaches. As a member of the Biometric Privacy Task Force, Ben is involved in the defense of class actions under BIPA and regularly works with clients on compliance and litigation. Staying up-to-date on domestic and international privacy laws, Ben provides

clients with the latest privacy law developments and performs legal research concerning cutting-edge privacy issues.

In his free time, Ben enjoys playing with his dog Remmy, hunting, fishing, watching sports and spearfishing.