EUROPE – GDPR IS HERE AND SO ARE THE FIRST GDPR COMPLAINTS

May 25th is now behind us and the European General Data Protection Regulation has now entered into effect.

Facebook and Google have already become the targets of the first official complaints of GDPR noncompliance, filed on the day the privacy law takes effect across the EU. Across four complaints, related to Facebook, Instagram, WhatsApp and Google’s Android operating system, European consumer rights organisation None Of Your Business (NOYB) argues that the companies have forced users into agreeing to new terms of service, in breach of the requirement in the law that such consent should be freely given. The group NOYB is headed up by none other than Max Schrems, the Austrian lawyer who has sued Facebook on multiple occasions.

Likewise, French digital rights group La Quadrature du Net has issued complaints against Google and Facebook, as well as Apple, Amazon, and LinkedIn. Google got separate complaints over Gmail, YouTube, and Search.

At the same time, some high-profile US news websites, such as The Chicago Tribune and LA Times, are currently unavailable in Europe following the entry of the GDPR. The following message on the Los Angeles Times when viewed in the EU: “Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.”

Read more:

The Guardian – Facebook and Google targeted as first GDPR complaints filed
EUROPE – EDPB GUIDELINES ON CERTIFICATION AND DEROGATIONS UNDER THE GDPR

On 30th May 2018, the European Data Protection Board (“EDPB”), which replaces the Article 29 Working Party, published the final version of Guidelines 2/2018 on derogations in the context of international data transfers pursuant to article 49 of the GDPR. These derogations are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards.

The EDPB also published draft Guidelines 1/2018 on certification under the GDPR. As per Article 42(3) of the GDPR, certification is a voluntary process to assist in demonstrating compliance with the GDPR. European member states and supervisory authorities are called to encourage the establishment of certification mechanisms and determine the stakeholder engagement in the certification process and lifecycle.

Read more:

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

EUROPE – EDPS PUBLISHES OPINION ON PRIVACY BY DESIGN

The European Data Protection Supervisor has published a preliminary opinion on the principle of privacy by design. According to the release, the opinion aims to raise awareness of data protection by design and by default as outlined by Article 25 of the GDPR. With this preliminary Opinion, the EDPS recalls the history of the principle of privacy by design within and outside the EU, from the initial research on privacy enhancing technologies (PETs) to the GDPR, provides examples of engineering methodologies and standardisation efforts and explores the meaning of privacy by design within the GDPR. The EDPS further calls on all stakeholders to join the dialogue on this issue.

Read more:

Preliminary Opinion on privacy by design

UNITED STATES – FTC APPROVES SETTLEMENT WITH PAYPAL REGARDING ALLEGED VENMO PRIVACY MISREPRESENTATIONS

The U.S. Federal Trade Commission has given final approval to a settlement with PayPal, Inc. over allegations that its Venmo peer-to-peer payment service misled consumers about their ability to transfer funds to external bank accounts and control the privacy of their Venmo transactions.

In its complaint, the FTC alleges that when Venmo notified users that money had been credited to their Venmo balances and was available for transfer to an external account, it failed to disclose that those funds could be
frozen or removed based on the results of Venmo’s review of the underlying transaction. The FTC also alleges that Venmo misled consumers about the extent to which they could control the privacy of their transactions. In addition, Venmo allegedly misrepresented the extent to which consumers’ financial accounts were protected by “bank grade security systems,” and violated the Gramm-Leach-Bliley Act’s Safeguards and Privacy Rules, according to the complaint.

As part of the settlement, Venmo is prohibited from misrepresenting any material restrictions on the use of its service, the extent of control provided by any privacy settings, and the extent to which Venmo implements or adheres to a particular level of security. Venmo also is required to make certain disclosures to consumers about its transaction and privacy practices and is prohibited from violating the Privacy Rule and the Safeguards Rule. Consistent with past cases involving violations of Gramm-Leach-Bliley Act Rules, Venmo is required to obtain biennial third-party assessments of its compliance with these rules for 10 years.

Read more:

Press Release – FTC Gives Final Approval to Settlement with PayPal Related to Allegations Involving its Venmo Peer-to-Peer Payment Service

**UNITED STATES – LOUISIANA UPDATES DATA SECURITY BREACH NOTIFICATION LAW**

On 20th May 2018, Louisiana Governor John Bel Edwards signed legislation S.B. 361 amending the state’s Database Security Breach Notification Law. The amended law provides new definitions, protects against the disclosure of personal information, requires specific security procedures and practices, details data breach notification requirements, and updates violations. The new law comes into effect on 1st August 2018.

Read more:

[LA S.B. 361](#)

**UNITED STATES - ARIZONA UPDATES DATA SECURITY BREACH NOTIFICATION LAW**

On 11th April 2018, Arizona Governor Doug Ducey signed legislation HB 2154 amending the state’s data breach notification law. The amended law will require persons, companies and government agencies doing business in the state to notify affected individuals within 45 days of determining that a breach has resulted in or is reasonably likely to result in substantial economic loss to affected individuals. The old law only required notification “*in the most expedient manner possible and without unreasonable delay.*” The amended law also broadens the definition of personal information and requires regulatory notice and notice to the consumer reporting agencies (“CRAs”) under certain circumstances. The new law comes into effect on 20th July 2018.

Read more:

[AZ HB 2154](#)

**NEW ZEALAND – NEW PRIVACY BILL EXAMINED IN PARLIAMENT**

New Zealand has a new privacy law on the way: a new Privacy Bill is currently being examined in Parliament with the objective to repeal and replace the current 25-year-old Privacy Act 1993. The stated purpose of the new
Privacy Bill is "to promote people's confidence that their personal information is secure and will be treated properly".

Read more:

[Newsroom - Is NZ’s new Privacy Bill a match for the EU’s GDPR?](#)

**CANADA - PRIVACY COMMISSIONER ISSUES GUIDELINES FOR CONSENT AND INAPPROPRIATE DATA PRACTICES**

On May 24, 2018, the Office of the Privacy Commissioner of Canada published two important guidance documents in respect of activities regulated pursuant to the Personal Information Protection and Electronic Documents Act ("PIPEDA"):

- Guidelines for Obtaining Meaningful Consent, which includes a checklist for consent and is effective on 1\textsuperscript{st} January 2019
- Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3), effective on 1\textsuperscript{st} July 2018

**UNITED STATES - FCC INVESTIGATING WEBSITE FLAW THAT EXPOSED MOBILE PHONE LOCATIONS**

According to Reuters, the U.S. Federal Communications Commission said it was referring reports that a website flaw could have allowed the location of mobile phone customers to be tracked to its enforcement bureau to investigate.

A security researcher found that data from LocationSmart, a California-based tech firm, could have been used to track AT&T, Verizon, Sprint and T-Mobile customers within a few hundred yards of their location and without their consent.

Senator Ron Wyden, an Oregon Democrat, on Friday had urged the FCC to investigate, saying on Twitter that a "hacker could have used this site to know when you were in your house so they would know when to rob it. A predator could have tracked your child’s cell phone to know when they were alone. I urge the FCC expand the scope of this investigation, and to more broadly probe the practice of third parties buying real-time location data on Americans,” Wyden said.

Robert Xiao, a researcher at Carnegie Mellon University, said a flaw in a demo tool from LocationSmart could have been used to track anyone.

Read more:

[Reuters – FCC investigating website flaw that exposed mobile phone locations](#)

**UPCOMING EVENTS**

Decoding the Numbers: The Latest in Cloud Standards
Businesses, government entities, and organizations continue to be drawn to the cloud. The cloud industry is still evolving frameworks for addressing cloud infrastructure, operations, risk management, security and interoperability of cloud services. The leading approach is by defining cloud security standards—industry-wide protocols that can be certified for a given cloud provider. The hope is that thorough and widely adopted cloud standards will foster further cloud adoption by providing cloud customers with evaluation tools.

The existing range of standards, where they are adopted at all, can be confusing to navigate. Standards bodies the world over share a love for names that read like a round of Scrabble. An alphabet soup of acronyms coupled with endless series of numbers has developed to identify existing and emerging standards related to cloud use and security. Read more here.

Ethics 101: Attorneys' Duties for Safeguarding Confidential Information on the Cloud

Most lawyers are using the cloud to store data even if they don’t realize it. Web-based e-mail is in the cloud. Office 365 data is in the cloud. Many of the software applications that lawyers rely on to run their practices are in the cloud.

But do clouds leak data? Assuredly they do, sometimes with scary regularity. No wonder lawyers worry about the potential ethical pitfalls of cloud computing, especially given the changes to ethical rules regarding competence with technology and the duty to safeguard confidential data. All attorneys seem to know that there is a prevailing reasonableness standard for vetting and using cloud providers, but lawyers struggle to understand what "reasonableness" means in the real world.

The panelists will explain the threats presented by cloud computing as well the benefits—and help you understand how to use cloud computing ethically. Read more here.

EDITORS

Paul Lanois - Mr Lanois is a global privacy, data protection and information security professional and is an attorney admitted to the Bars of the District of Columbia (DC-USA), New York (NY-USA) and the Supreme Court of the United States (SCOTUS). He regularly publishes articles on technology law and is frequently invited to speak on such topics. He has spoken at conferences across Europe, Asia and the United States. He was named a "Cybersecurity & Data Privacy Trailblazer" by the National Law Journal and an "Innovative Corporate Counsel" by Law 360. He was also recognized as a leading lawyer in The Legal 500’s GC Powerlist. He has been recognized as
a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional, with concentrations in Asian law (CIPP/A), US law (CIPP/US), European law (CIPP/E) and Canadian law (CIPP/C).

Nathan M. Barotz - Mr. Barotz has been in the private practice of law for over 25 years. A graduate of Duke University (cum laude) and the George Washington University Law School, Mr. Barotz originally developed a focus on health care law which in the last ten years has led to his strong interest the rapidly developing body of law governing IoT, cybersecurity and privacy. For the last five years, Mr. Barotz has served in the role of general counsel and compliance and privacy officer for companies utilizing telemedicine technology in post-acute patient treatment and currently serves in that role for HomeSleep, LLC, a company which specializes in diagnostic testing for sleep apnea. Mr. Barotz is a member of the New York State and Connecticut State Bars, the United States District Court Bars, Southern District and Eastern District of New York and has received his CIPP/US certification from the International Association of Privacy Professionals.

Tamara Lev - Ms. Lev is a Data Privacy attorney, specializing in: data security, information security, and regulatory compliance. She assists her clients with diligence and care, while identifying potential privacy vulnerabilities and conducting information security risk assessments. Tamara is a law graduate from Ono Academic College with a LLB in Law. She is a Fordham Law School graduate with a LLM in Intellectual Property and Information Technology. Tamara is a member of the State Bar of New York.

THOUGHTS? COMMENTS?

We are always looking to make this newsletter better, as such, we hope you like the new format of the newsletter. As always, comments and suggestions are always welcome. You can send your feedback to paulanocom@aol.com.

You are currently subscribed to the American Bar Association’s E-Privacy Law Committee mailing list. Your e-mail address will only be used within the ABA and its entities. We do not sell or rent e-mail addresses to anyone outside the ABA.

Update your profile | Unsubscribe | Privacy Policy

American Bar Association: 321 North Clark Street | Chicago, IL 60654 | 800-285-2221
Copyright © 2018 ABA, All Rights Reserved.