USA - UNIXIZ AGREES TO SETTLE CHARGES UNDER COPPA AND THE NEW JERSEY CONSUMER FRAUD ACT

On 3rd August 2018, a California-based company that ran a social media platform targeted at teenagers has agreed to shut down its fashion-themed social website for teens and reform its business practices to resolve allegations that the company violated state and federal laws by improperly collecting personal information from more than 2,500 New Jersey children and by failing to appropriately safeguard its users’ account information which was compromised in a 2016 data breach.

The authorities alleged that Unixiz, Inc., the company that owned and operated the online social website “i-Dressup”, violated the federal Children’s Online Privacy Protection Act (COPPA) and the New Jersey Consumer Fraud Act, by, among other things, failing to adequately safeguard user information and failing to obtain verifiable parental consent prior to collecting and processing children’s personal information.

“Children are extremely vulnerable on the internet and we must do all we can to protect them from being exploited by advertisers or tracked by internet predators,” said Attorney General Grewal. “We are committed to vigorously enforcing state and federal privacy protections and we will do everything we can to ensure that website operators comply with their duty to provide an extra layer of security on sites catering to young children.”

The allegations against Unixiz stem from an investigation initiated by the New Jersey Division of Consumer Affairs (the “Division”) after media outlets began reporting that the i-Dressup website had been breached by an unknown hacker and that user accounts were vulnerable.

The Division learned through its investigation that more than 24,000 of the compromised i-Dressup accounts belonged to New Jersey residents, 10,101 of whom were under the age of 18. The Division confirmed that 2,519 accounts belonged to children under the age of 13. The Division also alleged that Unixiz had improperly collected
personal information from the 2,519 children— including first and last names, email addresses, birthdates, and gender— without prior verifiable consent from their parents, as required by law.

In a Consent Order entered with the Division, Unixiz agreed to put in place measures to obtain verifiable parental consent on all company-operated websites that collect children’s information, as well as measures to provide parents with the ability to review the information that the company is collecting from their child, and to revoke the right of that company to collect or maintain their child’s information. Unixiz also agreed to implement policies and procedures to safeguard users’ account information.

The company also agreed to civil penalties in the amount of $98,618, $34,000 of which has been paid and $64,618 of which will be suspended and automatically vacated after two years, provided that the company complies with the terms of the Consent Order.

Read more: [Consent Order](#)

[Press Release - Operator of Teen Social Website Breached by Hacker Agrees to Close Site and Reform Practices to Settle Allegations it Violated Children’s Online Privacy Protection Act](#)

### USA - SEC CHARGES MIZUHO SECURITIES FOR FAILURE TO SAFEGUARD CUSTOMER INFORMATION

On 23 July 2018, the Securities and Exchange Commission (SEC) fined Mizuho Securities USA LLC for its failure to safeguard information pertaining to stock buybacks by its issuer customers.

According to the SEC, Mizuho failed to maintain and enforce policies and procedures aimed at preventing the misuse of material non-public information, including maintaining effective information barriers between different trading desks and requiring employees to keep client information confidential. Mizuho agreed to settle the charges and will pay a $1.25 million penalty.

The SEC’s order claims that, during a two-year period, Mizuho traders regularly disclosed material non-public customer buyback information to other traders and Mizuho’s hedge fund clients. That information included the identity of the party placing the order, the order size, limit price, and indications that the orders were buyback orders. The SEC further alleges that such information was routinely communicated across trading desks, notwithstanding that during the relevant period Mizuho executed over 99.8 percent of all buyback orders by using algorithms, rather than through trader-negotiated open market trades.

“Confidential information concerning issuer stock buybacks can be material to institutional investors, particularly when such trading comprises a significant portion of the daily trading volume in the stock being repurchased,” said Antonia Chion, Associate Director of the SEC Division of Enforcement. “Broker-dealers must be attentive to their responsibilities to maintain and enforce policies and procedures to prevent the misuse of such information.”

The SEC’s order finds that Mizuho wilfully violated Section 15(g) of the Securities Exchange Act of 1934. Without admitting or denying the SEC’s findings, Mizuho consented to the order imposing a $1.25 million penalty, a censure, and ordering it to cease and desist from committing or causing any future violations.

Read more: [Press Release - SEC Charges Mizuho Securities for Failure to Safeguard Customer Information](#)
EU / JAPAN – RECIPROCAL ADEQUACY DECISIONS ADOPTED

On 17 July 2018, the European Union and Japan agreed to recognise each other’s data protection systems as ‘equivalent’ and to adopt reciprocal adequacy decisions.

An adequacy decision is a decision taken by the European Commission establishing that a third country provides a comparable level of protection of personal data to that in the European Union, through its domestic law or its international commitments. As a result, personal data can flow safely from the European Economic Area (EEA) (the 28 EU Member States as well Norway, Liechtenstein and Iceland) to that third country, without being subject to any further safeguards or authorisations. This adequacy decision will concern the protections provided under the Japanese Act on the Protection of Personal Information. It will thus apply to all transfers of personal data to business operators in Japan. An adequacy decision is one of the tools provided for under the General Data Protection Regulation to transfer personal data from the EU to third countries. Even though the EU already has unilateral adequacy decisions with several other countries, this is the first time the EU and a third country agreed on a reciprocal recognition of the adequate level of data protection.

The future adequacy decisions will cover personal data exchanged for commercial purposes as well as personal data exchanged for law enforcement purposes between EU and Japanese authorities. In particular, the EU’s adequacy decision will concern the protections provided under the Japanese Act on the Protection of Personal Information and will thus apply to all transfers of personal data to business operators in Japan.

To align with European standards, Japan has committed to implementing the following additional safeguards to protect EU citizens’ personal data, before the Commission formally adopts its adequacy decision. These safeguards will bridge certain differences between the two data protection systems: for instance, the Japanese definition of sensitive data will be expanded, the exercise of individual rights will be facilitated, and the further transfer of Europeans’ data from Japan to another third country will be subject to a higher level of protection. Japan also agreed to establish a system of handling and resolution of complaints, under the supervision of the Japanese data protection authority (the Personal Information Protection Commission), to ensure that potential complaints from Europeans as regards access to their data by Japanese law enforcement and national security authorities will be effectively investigated and resolved.

The European Commission will shortly launch the process leading to the adoption of the adequacy decision under the General Data Protection Regulation. This includes obtaining an opinion from the European Data Protection Board, which brings together all of the national data protection authorities, and the green light from a committee comprised of representatives of the EU Member States. Once this procedure has been completed, the Commission will adopt the adequacy decision. The adequacy decision is therefore expected to be adopted in the last quarter of 2018 and should be applicable shortly after its adoption. Japan will also launch its relevant internal procedure for the adoption of its adequacy decision.

Source: Press Release - The European Union and Japan agreed to create the world's largest area of safe data flows

BRAZIL – NEW DATA PROTECTION LAW IS COMING TO BRAZIL

The Brazilian Congress has been working on a bill relating to the protection of personal data for over eight years. The Senate approved the bill, known as the General Data Protection Act (GDPA), on 10 July 2018, and the bill was sent to the President for execution. A window of 15 business days within which the President may veto the bill now follows. If the President does not actively reject the bill, it automatically becomes law. Thereafter, businesses
will have an 18-month grace period (i.e., up to and including 13 February 2020) to adjust to the change in law before it becomes effective on 14 February 2020.

The GDPA was motivated in part by Brazil’s desire to be admitted to the OECD and to prevent disruption in its commerce with the European Union and other important trading partners. As such, the GDPA seeks to match the level of protection afforded to data subjects by the laws of these trading partners.

The GDPA establishes rules on the collection, treatment, storage, and sharing of personal data, whether in digital or physical form. It provides various rights to data subjects, as well as a framework for private companies to develop their commercial activities. The GDPA has been greatly influenced by Europe’s General Data Protection Regulation (GDPR), but it also considers local sensibilities and certain best practices adopted by other countries in the area of data protection.

Read more: A New Era for Data Protection in Brazil

INDIA – NEW DRAFT DATA PROTECTION BILL ON THE WAY

On 27 July 2018, the Committee of Experts on Data Protection submitted to the Ministry of Electronics and Information Technology (MEITY) a draft Personal Data Protection Bill 2018 and a report on “A Free and Fair Digital Economy”.

The draft bill appears to be heavily inspired from the European General Data Protection Regulation which includes similar requirements, however the draft bill goes further and also includes, for example, a data localization clause.

No action is required at this stage since the bill is still in draft form: MEITY may of course accept, reject or alter such draft bill. The next step would be for the draft to be approved by the Union Cabinet before it is introduced in Parliament for deliberations. The final bill, if any, may therefore be very different from the current draft.

Here are the major proposals introduced by the draft bill:

• **Extra-territorial application**: Under Section 2, the draft bill would apply “to the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is — (a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or (b) in connection with any activity which involves profiling of data principals within the territory of India.”

• **Individuals’ rights**: The draft bill includes the “right to confirmation and access” (Section 24), the “right to correction” (Section 25), the “right to data portability” (Section 26) and the right to be forgotten (Section 27).

• **Transparency and accountability**: Chapter VII outlines transparency and accountability measures such as privacy by design (Section 29), data protection impact assessments (Section 33), record keeping (Section 34), data audits (Section 35) and the appointment of a Data Protection Officer (Section 36). Data protection impact assessments and data audits must be carried out by data fiduciaries which can be classified as significant data fiduciaries by the newly created Data Protection Authority. A mandatory registration requirement has been imposed on data processors who conduct “high risk processing”.

• **Data security**: Section 31 imposes the use of “appropriate security safeguards including (a) use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; and (c) steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.”
A mandatory data breach notification scheme is introduced under section 32, although no specific time frame for notification to the Data Protection Authority is provided.

- **Children’s rights**: A child is defined as someone who is less than 18 years of age. Profiling, tracking or behavioral monitoring of or targeted advertising towards children is not permitted.

- **Data Protection Authority**: Section 49 proposes the establishment of an independent Data Protection Authority of India (DPA). The DPA would oversee the monitoring and enforcing application of the bill, including the processing of data for reasonable purposes (Section 17), sensitive personal data (Section 22), data security breaches, data protection impact assessments (Section 33) and cross-border data transfers (Section 41).

- **Data localization**: Section 40 introduces restrictions on cross-border data flows, mandating that one serving copy of all personal data be stored in India: “Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies”. The central government is also empowered to classify any sensitive personal data as critical personal data and require its storage and processing only in India.

- **Cross-border data transfers**: In addition to consent, Section 41 states that cross-border data transfers require the use of model clauses or possible adequacy requirements, i.e. transfer to jurisdictions which have been approved by the government.

- **Sanctions**: Chapter XI (Section 69) provides maximum penalties of up to fifteen crore rupees (~ US$ 2,200,000) or four percent of the company's total worldwide turnover of the preceding financial year, whichever is higher. Certain criminal offences have been introduced, for example the obtaining, transferring or selling of personal data contrary to the Act can lead to imprisonment for a term of up to three years and a fine.

Read more: [Draft Personal Data Protection Bill 2018](#) and [Data Protection Committee Report](#)

## USA – FTC AMENDS PRIVACY ACT SYSTEM OF RECORDS NOTICES

The Federal Trade Commission (FTC) has adopted final amendments to its system of records notices under the Privacy Act of 1974 to ensure the Commission can disclose records to other agencies in the event of a data breach.

The Privacy Act of 1974 authorizes federal agencies to adopt routine uses of agency records subject to the Act as long as they are compatible with the purpose for which the information was collected. Acting on a recommendation from the President’s Identity Theft Task Force, the FTC in 2007 published a new routine use based on model language recommended from the Justice Department that allowed for disclosure of records to appropriate persons and entities in order to respond to a data breach. Since then, the Office of Management and Budget (OMB) determined that the model language was too narrow and that agencies needed authority to make disclosures that go beyond those contemplated by the original routine use.

Based on additional guidance provided last year by OMB, the final amendments approved by the Commission will be published in the Federal Register shortly. The final amendments more specifically address that harm to individuals may justify a routine use disclosure, and add a second routine use to allow the FTC to disclose information to another federal agency when it is reasonably needed to respond to a breach.

Read more: [Press Release - FTC Amends Privacy Act System of Records Notices](#)
EU - EUROPEAN DATA PROTECTION BOARD LETTER TO ICANN

The European Data Protection Board (EDPB) adopted a letter on behalf of the EDPB Chair addressed to the Internet Corporation for Assigned Names and Numbers (ICANN), providing guidance to enable ICANN to develop a GDPR-compliant model for access to personal data processed in the context of WHOIS.

The letter addresses the issues of purpose specification, collection of “full WHOIS data”, registration of legal persons, logging of access to non-public WHOIS data, data retention and codes of conduct and accreditation.

The EDPB’s predecessor, WP29, has been offering guidance to ICANN on how to bring WHOIS in compliance with European data protection law since 2003.

The EDPB expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.

Read more: European Data Protection Board letter to ICANN

EU – CROSS-BORDER COOPERATION AND CONSISTENCY PROCEDURES: STATE OF PLAY

During its second plenary meeting on 4 and 5 July, the European Data Protection Board (EDPB) discussed the consistency and the cooperation systems, sharing first experiences on the functioning of the One-Stop Shop mechanism, the performance of the Internal Market Information System (IMI), the challenges the authorities are facing and the type of questions received since 25 May. Most data protection authorities reported a substantial increase in complaints received. The first cross-border cases were initiated in IMI on 25 May. Currently, around 100 cross-border cases in IMI are under investigation.

The EDPB Chair Andrea Jelinek said: “Despite the sharp increase in the number of cases in the last month, the Members of the EDPB report that the workload is manageable for the moment, in large part thanks to a thorough preparation in the past two years by the Article 29 Data Protection Working Party. However, we should only expect the first results of the new procedures to deal with cross-border cases in a few months from now. To handle complaints, lead supervisory authorities will have to carry out investigations, observe procedural rules, and coordinate and share information with other supervisory authorities. The GDPR sets specific deadlines for each phase of the procedure. All of this takes time. During this time, complainants are entitled to be kept informed on the state of play of a case. The GDPR does not offer a quick fix in case of a complaint but we are confident the procedures detailing the way in which the authorities work together are robust and efficient.”

USA - CALIFORNIA COMPANY SETTLES FTC CHARGES RELATED TO PRIVACY SHIELD PARTICIPATION

A California company has agreed to settle Federal Trade Commission allegations that it falsely claimed it was in the process of being certified as complying with the EU-U.S. Privacy Shield framework, which establishes a process to allow companies to transfer consumer data from European Union countries to the United States in compliance with EU law.

“Today’s settlement demonstrates the FTC’s continuing commitment to vigorous enforcement of the Privacy Shield,” FTC Chairman Joe Simons commented. “We believe Privacy Shield is a critical tool for ensuring transatlantic data flows and protecting privacy that benefits both companies and consumers.”
According to the FTC’s complaint, the Commission alleges that ReadyTech Corporation, which provides online training services, falsely claimed on its website that it is “in the process of certifying that we comply with the U.S.-E.U. Privacy Shield Framework.” While ReadyTech initiated an application to the U.S. Department of Commerce in October 2016, the company did not complete the steps necessary to participate in the Privacy Shield framework. The Department of Commerce administers the framework, while the FTC enforces the promises companies make when joining the Privacy Shield.

The FTC alleges in its complaint that the company’s false claim that it is in the process of certification violates the FTC Act’s prohibition against deceptive acts or practices.

As part of the settlement, ReadyTech is prohibited from misrepresenting its participation in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework and the Swiss-U.S. Privacy Shield framework. It also must comply with standard reporting and compliance requirements.

This is the FTC’s fourth case enforcing Privacy Shield. It continues the FTC’s commitment to enforcing international privacy frameworks, making a total of 47 cases enforcing the Privacy Shield, the predecessor Safe Harbor framework, and the Asia Pacific Economic Cooperation Cross Border Privacy Rules framework.

Read more: Press Release - California Company Settles FTC Charges Related to Privacy Shield Participation

EU – PARLIAMENT CALLS ON THE EU COMMISSION TO SUSPEND THE PRIVACY SHIELD

MEPs call on the EU Commission to suspend the EU-US Privacy Shield as it fails to provide enough data protection for EU citizens.

The data exchange deal should be suspended unless the US complies with EU data protection rules by 1 September 2018, say MEPs in a resolution passed on Thursday by 303 votes to 223, with 29 abstentions. MEPs add that the deal should remain suspended until the US authorities comply with its terms in full.

Following the Facebook-Cambridge Analytica data breach, MEPs emphasize the need for better monitoring of the agreement, given that both companies are certified under the Privacy Shield.

MEPs call on the US authorities to act upon such revelations without delay and if necessary to remove companies that have misused personal data from the Privacy Shield list. EU authorities should also investigate such cases and if appropriate, suspend or ban data transfers under the Privacy Shield, they add.

MEPs are worried that data breaches may pose a threat to democratic processes if data is used to manipulate political opinion or voting behaviour.

MEPs are also worried about the recent adoption of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), a US law that grants the US and foreign police access to personal data across borders.

They point out that the US law could have serious implications for the EU and could conflict with EU data protection laws.

Civil Liberties Committee Chair and rapporteur Claude Moraes (S&D, UK) said: "This resolution makes clear that the Privacy Shield in its current form does not provide the adequate level of protection required by EU data
protection law and the EU Charter. Progress has been made to improve on the Safe Harbor agreement but this is insufficient to ensure the legal certainty required for the transfer of personal data.”

"In the wake of data breaches like the Facebook and Cambridge Analytica scandal, it is more important than ever to protect our fundamental right to data protection and to ensure consumer trust. The law is clear and, as set out in the GDPR, if the agreement is not adequate, and if the US authorities fail to comply with its terms, then it must be suspended until they do.”

Read more: European Parliament resolution on the adequacy of the protection afforded by the EU-US Privacy Shield

NETHERLANDS - DUTCH SUPERVISORY AUTHORITY ANNOUNCES GDPR INVESTIGATION

On 17th July 2018, the Dutch Supervisory Authority announced that it will start a preliminary investigation to assess whether certain large corporations comply with the new European privacy requirements (the GDPR). It further announced that it will review the “records of processing activities” from thirty randomly selected corporations which are located in the Netherlands.

Article 30 of the GDPR requires data controllers and processors to maintain a record of their processing activities, however the record of processing activities does not apply ‘to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.’

Read more: Press Release (in Dutch)

FRANCE – FRENCH SUPERVISORY AUTHORITY ISSUES 2 GDPR WARNINGS

On 19th July 2018, the French Supervisory Authority (CNIL) announced that it has issued a formal warning to two companies in relation to their processing of localization data for targeted advertising. It found that consent was not validly obtained by both companies and that one company was keeping location data longer than necessary.

Two marketing companies, Fidzup and Teemo, offer a tool (SDK) that allows their customers, mobile app operators, to collect geolocation data and to use this data to provide customized advertising to their app users. The companies provide tools integrated into the mobile application code of their partners. They allow them to collect data from smartphone users even when these applications are not running.

The SDK tool provided by Teemo allowed partner companies to collect the advertising ID of the smartphones and the geolocation data of customers every five minutes. The data is then linked to points of interest determined by partner companies (e.g. store signs), who can display targeted advertising on people's smartphones based on places visited.

Fidzup on the other hand provides a SDK tool which allow application partners to collect mobile advertising identifiers and the MAC address of the smartphone, and also installs "FIDBOX" devices in various sales outlets to collect data on the MAC address and the WIFI signal strength of smartphones. The data collected are then linked together, allowing the company to carry out targeted advertising based on individual’s smartphone location when they pass close to a FIDZUP point of sale.
The CNIL found, in relation to Teemo that individuals were not informed, when downloading an app that a tool is used to collect their data, including location data. In relation to Fidzup, the CNIL found that customers were not informed of the purpose of the processing giving rise to the targeted advertising, nor of the identity of the person responsible for this treatment. In addition, the information provided to customers on posters in stores takes place after the collection and the processing of the data, whereas the consent requires prior notice.

Moreover, the CNIL found that both companies do not allow customers to download a version of the mobile application without the SDK tool. The use of the applications automatically results in the transmission of data to companies. Finally, the CNIL found that if customers were actually asked to consent to the processing of their geolocation data during the installation of mobile applications, this action only relates to the use of data by such application, not consent to the collection of data for advertising purposes via the SDK tool. The CNIL therefore concluded that the consent obtained did not meet the requirements of the GDPR.

The CNIL also found that Teemo proposes to keep location data for 13 months, which the CNIL found is contrary to the obligation to define and respect a data retention period proportionate to the purpose of the processing. The CNIL emphasized that location data can only be kept for a period strictly proportionate to the purpose of the processing that justified location tracking, which was not the case here.

Read more: Press Release - Mobile applications: formal notice for lack of consent to geolocation data processing for advertising targeting purposes (in French)

UPCOMING EVENTS

Best Practices for Handling Data Privacy and Cybersecurity in M&A

Format: Webinar
Date: August 21, 2018
Time: 1:00 PM - 2:30 PM ET
Credits: 1.50 General CLE Credit Hours
Panelists: Gerard M Stegmaier, Jane Rosen, Jennifer C Archie

Expert panelists will discuss and analyze the changes in the cybersecurity and privacy landscape for M&A transactions and provide best practices practitioners can consider for identifying, managing, and mitigating data privacy and cybersecurity risks in handling M&A transactions.

Significant changes have arisen in market expectations on the handling of privacy and cybersecurity risks in merger and acquisitions (M&A) transactions. The changes have resulted from the dramatic increase in devastating cyberattacks and from the growing number of legislative measures addressing privacy and cybersecurity and the focus of regulators on these issues, including in their review of M&A deals. Thorough and substantive diligence in these areas is imperative. Read more here.

While You Were Sleeping: Ever-Changing Cybersecurity Threats and What You Need to Know Now

Format: Webinar
Date: August 22, 2018
Businesses of all kinds (including law firms) are facing unprecedented challenges from cyber-attacks. The 2016 presidential race revealed how hacktivists and enterprising criminal actors can wreak havoc with databases and business firewalls to make political statements, influence elections, or plunder proprietary data. Ransomware can hold companies, law firms, driverless cars, medical devices, and even law enforcement agencies hostage. Business Email Compromise (BEC), the sophisticated scam that compromises legitimate email accounts through social engineering and computer intrusion techniques, has resulted in unauthorized transfers of funds ($3.1 billion and counting) from businesses that work with foreign suppliers.

From the massive Panama Papers breach that seriously affected the Mossack Fonseca law firm in 2016, to the Equifax data breach and WannaCry and Petya/NotPetya ransomware attacks in June 2017, cyber-attacks have become a real and direct threat to law practices and their clients.

As mobile devices, social media, the Internet of Things, cloud computing, big data analytics, and the latest disruptive technologies dramatically change the way we communicate and do business, corporations, government entities, and law firms are taking on levels of risk they may not understand.

Cybersecurity Is Not One Size Fits All: Addressing Night and Day Differences for Solos/Small Firms, Megafirms, Companies, Government, and Nonprofits

All lawyers face cybersecurity challenges, regardless of their practice setting or organization size. It does not matter if you have no IT department or designated budget, every lawyer and every business must address cybersecurity risks. Companies, law firms (from solo to megafirm), nonprofits, and government entities are all targets, and no one is safe. But cybersecurity is not one size fits all. Join us to hear perspectives from seasoned cybersecurity practitioners with a wide range of experience in different practice settings.
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.

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.