UNITED STATES – ALTABA (FORMERLY KNOWN AS YAHOO!) CHARGED WITH FAILING TO DISCLOSE CYBERSECURITY BREACH AND FINED $35 MILLION

On 24 April 2018, the Securities and Exchange Commission announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world’s largest data breaches in which hackers stole personal data relating to hundreds of millions of users’ accounts.

According to the SEC’s order, within days of the December 2014 intrusion, Yahoo’s information security team learned that Russian hackers had stolen what the security team referred to internally as the company’s “crown jewels”: usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of users’ accounts. Although information relating to the breach was reported to members of Yahoo’s senior management and legal department, Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors. The fact of the breach was not disclosed to the investing public until more than two years later, when in 2016 Yahoo was in the process of closing the acquisition of its operating business by Verizon Communications, Inc.

“We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company’s response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case,” said Steven Peikin, Co-Director of the SEC Enforcement Division.

Jina Choi, Director of the SEC’s San Francisco Regional Office, added, “Yahoo’s failure to have controls and procedures in place to assess its cyber-disclosure obligations ended up leaving its investors totally in the dark about a massive data breach. Public companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors.”
The SEC’s order finds that when Yahoo filed several quarterly and annual reports during the two-year period following the breach, the company failed to disclose the breach or its potential business impact and legal implications. Instead, the company’s SEC filings stated that it faced only the risk of, and negative effects that might flow from, data breaches. In addition, the SEC’s order found that Yahoo did not share information regarding the breach with its auditors or outside counsel in order to assess the company’s disclosure obligations in its public filings. Finally, the SEC’s order finds that Yahoo failed to maintain disclosure controls and procedures designed to ensure that reports from Yahoo’s information security team concerning cyber breaches, or the risk of such breaches, were properly and timely assessed for potential disclosure.


**UNITED STATES – FTC WARNS FOREIGN COMPANIES OVER ALLEGED COPPA VIOLATIONS**

The staff of the Federal Trade Commission sent letters to two foreign companies that market electronic devices and apps that appear to collect geolocation data from children, warning that the companies may be in violation of the Children’s Online Privacy Protection Act (COPPA) Rule.

The letters were sent to China-based Gator Group Co., Ltd., and Sweden-based Tinitell, Inc., which both provide online services. Gator Group advertises an app and a device called the Kids GPS Gator Watch, which it markets as a “child’s first cell phone.” Tinitell has also marketed an app that works with a mobile phone worn like a watch, which is also designed for children. Although Tinitell has stopped selling the devices, they will continue to operate through September 2018. Copies of the letters were also sent to the Apple App Store and the Google Play Store, which make the apps available to consumers in their stores.

The FTC’s COPPA Rule requires companies collecting personal information from children under the age of 13 to post clear privacy policies and to notify parents and get their consent before collecting, using or sharing personal information from a child.

In its letters to the two companies, the FTC noted that even though they are based outside the United States, foreign companies are required to comply with COPPA when their services are directed to children in the United States or they knowingly collect information from U.S.-based children.

The online services offered by both companies appear to be directed to children and to collect precise geolocation information from children. The letters note that a review of both companies’ services reveal that they do not appear to provide direct notice of their collection practices and do not seek verifiable parental consent before collecting, using or disclosing personal information as required by COPPA. The letters encourage the companies to review their online services, policies and procedures to ensure they are in compliance with COPPA.


**UNITED STATES – MOBILE PHONE MAKER BLU REACHES SETTLEMENT WITH FTC OVER DECEPTIVE PRIVACY AND DATA SECURITY CLAIMS**

Mobile phone manufacturer BLU Products, Inc. and its co-owner have reached a settlement with the Federal Trade Commission over allegations that the company allowed a China-based third-party service provider to collect detailed personal information about consumers, such as text message contents and real-time location
information, without their knowledge or consent despite promises by the company that it would keep such information secure and private. As part of the settlement, BLU must implement a comprehensive data security program to help prevent unauthorized access of consumers’ personal information and address security risks related to BLU phones.

In its complaint, the FTC alleges that BLU and its co-owner and President Samuel Ohev-Zion misled consumers by falsely claiming that they limited third-party collection of data from users of BLU’s devices to only information needed to perform requested services. They also falsely represented that they had implemented “appropriate” physical, electronic, and managerial procedures to protect consumers’ personal information, according to the FTC complaint.

According to the FTC complaint, Florida-based BLU contracted with ADUPS Technology Co. LTD to issue security and operating system updates to BLU’s devices. ADUPS, however, collected and transferred to its servers more information than needed to do its job, including the full content of consumers’ text messages, real-time location data, call and text message logs with full telephone numbers, contact lists, and lists of applications used and installed on BLU devices.

The FTC complaint further states that BLU and Ohev-Zion failed to implement appropriate security procedures to oversee the security practices of their service providers, including failing to perform appropriate due diligence of service providers; failing to have written data security procedures regarding service providers; and failing to adequately assess the privacy and security risks of third-party software installed on BLU devices. As a result, ADUPS collected sensitive personal information via BLU devices without consumers’ knowledge and consent that it did not need to perform its contracted services. In addition, ADUPS software preinstalled on BLU devices contained common security vulnerabilities that could enable attackers to gain full access to the devices.

After reports about the unexpected collection and sharing by ADUPS became public in November 2016, BLU issued a statement informing consumers that ADUPS had updated its software and had stopped its unexpected data collection practices. Despite this, the FTC alleges that BLU continued to allow ADUPS to operate on its older devices without adequate oversight.

Under the proposed settlement with the FTC, BLU and Ohev-Zion are prohibited from misrepresenting the extent to which they protect the privacy and security of personal information and must implement and maintain a comprehensive security program that addresses security risks associated with new and existing mobile devices and protects consumer information. In addition, BLU will be subject to third-party assessments of its security program every two years for 20 years as well as record keeping and compliance monitoring requirements.

Read more: [Mobile Phone Maker BLU Reaches Settlement with FTC over Deceptive Privacy and Data Security Claims](#)

**UNITED STATES - OREGON ENACTS STRICTER DATA BREACH LAW**

As news of data breaches becomes more and more common, Oregon Governor Kate Brown has signed legislation which will require that residents be notified within 45 days after a data breach has been discovered, unless doing so would impede a law enforcement investigation. The law, which will take effect in June, will also prohibit credit reporting agencies from charging a fee to residents who want to freeze or unfreeze their credit reports.

In March, Washington state Governor Jay Inslee signed a no-fee credit freeze bill into law. As reported in our newsletter last month, South Dakota Governor Dennis Daugaard signed on March 21 that state’s first data breach
notification law, which takes effect July 1. That law requires organizations and agencies to information data breach victims within 60 days of breach discovery or notification by a third party. Then in April, the Alabama Data Breach Notification Act of 2018 was passed, making it the 50th and final U.S. state to enact a data breach notification law.

Read more:

SB 1551 - Oregon Legislative Information System
SciTech E-Privacy Newsletter - March 2018 issue

UNITED STATES - CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT

On March 23 President Trump signed into law the Clarifying Lawful Overseas Use of Data Act (the “Act”) which amends the Stored Communications Act (the “SCA”) to require providers of electronic communication services or remote computing services to produce data sought by the government under the SCA regardless of whether the data are located within or outside the United States. The Act clarifies provider obligations to produce foreign-stored data to U.S. law enforcement agencies as well as establishing a framework that may allow service providers to disclose communications to certain foreign governments.

The Act expressly requires providers to comply with the SCA's data retention and disclosure obligations regardless of where the data are stored. It states that providers must "comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

The Act also provides a mechanism for certain service providers to challenge a warrant issued under the SCA in some cases. A provider of electronic communication service "to the public" or remote computing service may move to quash or modify the warrant if the provider reasonably believes: (1) that the customer or subscriber is not "a United States person" and does not reside in the United States; and (2) that the disclosure would "create a material risk that the provider would violate the laws of a "qualifying foreign government."

The Act does not, however, provide a mechanism to challenge warrants or other legal process requesting data of targets who are United States persons or residents. Nor does it authorize providers to challenge warrants that would require them to violate the laws of a foreign country that is not a "qualifying foreign government."

The Act also establishes a framework for "qualifying foreign governments," as defined in the ACT, to request data stored in the United States.

Read more: S.2383 — 115th Congress (2017-2018)

UNITED STATES - PRIVACY LAW SPECIALIST CERTIFICATION

As what some might see as a reflection of the growing importance of privacy law in an increasingly technological world, in February and the American Bar Association's House of Delegates voted to approve a resolution on the International Association of Privacy Professionals’ designation of “Privacy Law Specialist” for a five-year term. Privacy Law is the 15th specialty accredited by the ABA.
Under U.S. law, attorneys have the right to advertise that they specialize in a particular field of law if they are certified as such by a “bona fide” organization. The approval is intended to authorize lawyers to list the designation alongside their name on their business cards, online profiles, professional websites, or email signature lines, while complying with the Model Rules of Professional Conduct provisions on Communication of Fields of Practice and Specialization.

“With this vote, lawyers who wish to distinguish themselves from the crowd and demonstrate to potential employers or clients that they have taken extra steps to develop privacy law credentials have an opportunity to do so,” said IAPP Research Director Rita Heimes, CIPP/E, CIPP/US, CIPM. "The IAPP is proud to be acknowledged by the ABA as an accredited provider of the Privacy Law Specialist certification."

Read more: IAPP - Privacy Law Specialist

**UNITED STATES - FEDERAL RULES OF CIVIL PROCEDURE TRUMP E.U. DATA DIRECTIVE IN CIVIL LITIGATION DISCOVERY**


Email communication and ESI have become a common form of communication in world commerce, yet the United States and the European Union have applied different default rules concerning its ownership and placed different default rules on their use in litigation. The European Union considers any email or ESI which contains a personal identifier, such as a name, to contain personal data. The EU Data Protection Directive (also known as Directive 95/46/EC) is a regulation adopted by the European Union to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using or exchanging such data.

As it relates to litigation, the EU Data Protection Directive forbids production of any emails or ESI without first identifying the individuals whose “personal data” is implicated and obtaining the consent to its disclosure. In practice, these rules dramatically reduce the exchange of documents between parties in European litigation.

In dismissing the concerns raised by such a U.S. company and ordering it to produce ESI in the U.S. which was stored in the E.U., the court considered the following five factors: “(1) the importance to the litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.”

In addition, the Court stated that the “defendant’s concerns premised on other German statutes that impose civil and criminal penalties for violations of the Data Protection Act are not sufficient to move this Court to disregard its duty to render a fully informed disposition of this case, particularly where a sensible construction of the statute in question reveals that the disclosure would not violate the Act, and the defendant has not pointed to any information to suggest that it faces any plausible risk of an enforcement action by German authorities.”
EUROPEAN UNION - FINAL GUIDELINES ON CONSENT AND TRANSPARENCY PUBLISHED

The Article 29 Working Party, composed of representatives of the national data protection authorities in the European Union, has published final guidelines on consent and transparency under the GDPR. In addition, it has issued a statement on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU. Last but not least, it has published a position paper in relation to the derogations to the obligation, under article 30 of the GDPR, for controllers and processors to maintain a record of processing activities.

Read more:

Guidelines on Consent under Regulation 2016/679
Guidelines on Transparency under Regulation 2016/679
Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU
Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) of the GDPR

CANADA: BREACH NOTIFICATION REQUIREMENT TO COME INTO FORCE IN NOVEMBER

On March 26, 2018, the Canadian government announced that, on November 1, 2018, important changes to the Personal Information Protection and Electronic Documents Act (PIPEDA) will come into force.

Among other things, the changes will require domestic and foreign organizations subject to PIPEDA to: (a) notify individuals about privacy breaches; (b) report privacy breaches to the Office of the Privacy Commissioner of Canada and others in certain circumstances; and (c) keep certain records of privacy breaches.

Read more: Canadian Privacy Breach Notification Rules in Force on November 1, 2018

HONG KONG: UPDATE TO ITS DATA PROTECTION LAW MAY BE COMING SOON FOLLOWING ‘MAJOR DATA LEAKS’

The head of Hong Kong’s data privacy watchdog said last week that he would review Hong Kong’s existing data protection law following a series of “major data leaks” in the city that affected more than half a million people.

As well as a recent hack into an inactive database owned by Hong Kong Broadband Network (HKBN) that held information on 380,000 customers, a number of cyberattacks also targeted databases belonging to travel agencies, involving some 220,000 clients. Private information such as credit card details, home addresses, names and ID card numbers could have been compromised in the hacks.
Speaking on an online programme hosted by former lawmaker Emily Lau Wai-hing, Privacy Commissioner for Personal Data Stephen Wong Kai-yi said it was time to review the Personal Data (Privacy) Ordinance, which came into force in 1996. The legislation was last updated in 2012, but with a focus only on direct marketing.

“The European Union has a new regulation next month, we also see some major data leaks in Hong Kong and [on an] international level ... I think it is time,” Wong said. The commissioner said his office would study if enough protection was provided to citizens, and also look at global trends.

Wong said the city’s ordinance was based on the EU’s Data Protection Directive, due to be replaced by the General Data Protection Regulation next month. The commissioner also admitted his office’s enforcement power was lower than other regulatory bodies in other countries. “Lawmakers think our enforcement power has to be increased. I see their point,” Wong said.

Read more: Hong Kong’s privacy commissioner to review ageing data protection law after ‘major data leaks’

THAILAND: EXTRATERRITORIAL APPLICABILITY INTRODUCED IN NEW DRAFT PERSONAL DATA PROTECTION BILL

The Ministry of Digital Economy and Society in Thailand has published a revised version of the draft Personal Data Protection Bill (“Amended PDPB”) in early April 2018.

Among the new concepts introduced in the draft is the concept of extraterritorial application. Data controllers and data processors, both located in Thailand and overseas, will be subject to the requirements under the Amended PDPB for the collection, use or disclosure of personal data occurring in Thailand.

Data controllers and data processors who collect, use, or disclose personal data outside Thailand but (1) any parts of such actions occurred in Thailand; or (2) the consequence of such actions intentionally to be occurred in Thailand; or (3) the consequence of such action should occur or it could be foreseen that the consequence would occur in Thailand, will be subject to the Amended PDPB.

If this is kept in the final version of the Bill, this could mean that any organization located overseas, especially online service providers, who collect, use, or disclose personal data of or provides services to individuals in Thailand may be subject to the requirements under the Amended PDPB. Having any part of a network, data centers or servers in Thailand could also result in being subject to the Amended PDPB.

Read more: New Draft Thai Personal Data Protection Bill - Extraterritorial Applicability Introduced

VIETNAM: NEW LAW ON CYBER-SECURITY TO COME

It is expected that a new Law on Cyber-Security will be debated and adopted at the May 2018 session of Vietnam’s National Assembly. Since the release of the first draft in June 2017, the drafting committee has continued to fine tune the draft law to provide principles, measures, and activities to ensure the implementation of cybersecurity tasks; the responsibilities of relevant agencies, organisations, and individuals in management positions, providing services in cyberspace, and using cyberspace; and the protection of cybersecurity in Vietnam.
What may be the most significant change in the draft law is the removal of offshore entities' requirement of having local servers in Vietnam.

However, article 27.4 of the draft law imposes on offshore entities providing telecommunications and Internet services in Vietnam the following:

- If (i) 10,000 or more Vietnamese users use their service, or if (ii) the Government so requests, such offshore entities must:
  - Have headquarters or representative offices in Vietnam; and
  - Store within Vietnam (i) the data of Vietnamese users, and (ii) other important data collected and/or generated from the use of Vietnam's national cyber infrastructure;
- Fulfil requirements provided by the competent Vietnamese authorities about the prevention and removal of information that infringes national security, social order and safety and legitimate rights and interests of organizations and individuals; provide Vietnamese users’ data upon request and deal with matters in violation of the Cybersecurity Law.

The draft law is, however, still subject to further review and adjustments.

Read more: New Cyber-Security Law to Be Considered by Vietnam’s National Assembly

UPCOMING EVENTS

Internet of Things National Institute

Format: In-Person
Location: Crowell & Moring LLP
Date: May 9-10, 2018
Credits: 13.25 General CLE Credit Hours, 1.00 Ethics/Professionalism CLE Credit Hours

The Internet of Things (IOT) is defined as billions of vehicles, buildings, process control devices, wearables, medical devices, drones, consumer/business products, mobile phones, tablets, and other “smart” objects that are wirelessly connecting to and communicating with each other. This new top law practice area is raising unprecedented legal and liability issues.

As one of the most transformative and fast-paced technology developments in recent years, IoT will require businesses, policymakers, and lawyers (M&A, IP, competition, litigation, health law, IT/outsourcing, and privacy/cybersecurity) to identify and address the escalating legal risks of doing business in a connected world.

Attend this institute to:

- Discover why corporate, law firm, government, university, and other attendees gave the last two IoT Institutes rave reviews, calling it “magical,” “eye-opening,” with “rock star” speakers, and overall “a grand slam.”
- Gain insights and practical guidance on the latest legal, legislative, regulatory, and liability issues of the IoT transformation—a game-changer for businesses, policymakers, and lawyers that’s generating hundreds of billions of dollars in spending globally.
- Explore need-to-know IoT hot topics: big data/privacy, cybersecurity, litigation/mitigation, cloud/artificial intelligence, connected healthcare, ethics, global IoT product development and sales, insurance risk allocation, and homeland/national security.
• Get great value: Two (2) days of CLE credit (including ethics), including three (3) keynotes packed with compelling perspectives. There will also be opportunities for networking. Read more here.

Cyberinsurance: Necessary, Expensive and Confusing as HeckABA Value Pass

Format: Webinar
Date: May 22, 2018
Time: 1:00 PM - 2:00 PM ET
Credits: 1.00 General CLE Credit Hours
Panelist(s): Judith Selby, Sharon D Nelson

Learn the basics of cyberinsurance, what gets covered, the costs, and the pros and cons of buying it. It seems like a new data breach occurs every week. Although you already have insurance, don’t be fooled into thinking that your general liability coverage protects you from a cyber incident. Cyberinsurance can cover the destruction or theft of your confidential client information—but do you really need it? 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