Foreword

Dear Readers,

This Saturday marks the 10th anniversary for Data Protection Day, celebrated each year on 28 January – which is the date the Council of Europe’s data protection convention, known as “Convention 108”, was established. Data Protection Day, known as Privacy Day outside of Europe, is now celebrated globally, raising awareness of people’s rights as they relate to the automatic processing of their data.

In addition to the 10-year milestone, Data Protection Day is particularly noteworthy this year as organizations around the world grapple with the European Union’s (EU) General Data Protection Regulation (GDPR). The regulation, which passed this time last year, gave everyone two and half years to come to grips with and put into place the measures needed for compliance. With one of those years now behind us, GDPR is teaching us a lot about company attitudes in this area. There appears to be little progress on the compliance effort to date, as poor acceptance of accountability across organizations suggests a belief that the task ahead is one for the specialists – either legal or technical. For those of you who are not completely familiar with the GDPR, the (ISC)² EAC GDPR Task Force has published an overview of the basics that can be used as a tool to help everyone understand and communicate the scope of what is required.

Please find below the latest edition of the SciTech E-Privacy Law Committee Newsletter. Please do not hesitate to contact us with any comments, questions, ideas or contributions you may have for this newsletter.

Paul Lanois
Editor
paulanocom@aol.com

News

EU proposal for regulation on privacy and electronic communications

On 10 January 2017, the European Commission published a proposed Regulation on Privacy and Electronic Communications concerning the protection of privacy and personal data in the electronic communications sector, designed to increase the protection of people’s private life and to open up new opportunities for business. The aim is to bring
the regulations up to date and to align e-privacy laws within the new European data protection framework (including the EU General Data Protection Regulation), as part of the strategy for a Digital Single Market.

The draft regulation includes enhanced privacy measures, including in relation to user consent, confidentiality of electronic communications, website cookies and unsolicited electronic communications, and introduces an enforcement regime in line with the GDPR, with the potential for significant fines for breaches.

The privacy rules would cover new providers of electronic communications services, such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, and Viber. It is also envisaged to simplify the applicable rules on cookies.

The Commission says that it is hoping that the new rules can be adopted by 25 May 2018, when the General Data Protection Regulation comes in to force.

Read more:

European Commission Press Release - Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions

Theresa May sets out plan for Brexit

Prime Minister Theresa May has outlined her plans for Brexit, making it clear that the UK will withdraw from both the European Union and the single market - but that the government will continue to try and attract "potential, talent and ambition" following the UK's departure from the EU. It was further clarified that existing EU laws in force in the UK would be converted into full UK laws, confirming that the EU's General Data Protection Regulation will also be law in the UK.

Read more:

V3 - Brexit: Theresa May sets out plan to make UK "the best place for science and innovation"

EU to begin adequacy discussions with Japan, Korea and Latin American countries

The EU Commission has indicated that it will proactively engage in discussions on reaching "adequacy decisions" (allowing for the free flow of personal data to countries with "essentially equivalent" data protection rules to those in the EU) with key trading partners in East and South-East Asia, starting with Japan and Korea in 2017, but also with interested countries of Latin America and the European Neighbourhood.

Read more:
European Commission Press Release - Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions

The rising cost of data breaches

A recent IBM study found that the average cost of a data breach has hit $4 million - up from $3.8 million in 2015. The study also reports that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased from $154 to $158. In addition to cost data, the global study puts the likelihood of a material data breach involving 10,000 lost or stolen records in the next 24 months at 26 percent. Things are not going to ease up anytime soon: as security intelligence provider Risk Based Security points out in its 2016 Data Breach Trends report, "six 2016 breaches have taken their place on the Top 10 List of All Time Largest Breaches."

Read more:
IBM - Cost of Data Breach Study

CSO Online - Top data breach trends in 2016: Phishing, skimming rise; hacking holds ground

President's Trump executive order on the application of the federal Privacy Act

The new executive order, titled "Enhancing Public Safety in the Interior of the United States," includes a provision that is meant to impact the privacy practices of U.S. agencies with regard to the personal data of noncitizens. Its section 14 states the following: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."

Some have stated that this presidential order could wreck US-EU Privacy Shield. Member of the European Parliament Jan Philipp Albrecht feared the order would undermine the Privacy Shield and tweeted "If this is true @EU_Commission has to immediately suspend #PrivacyShield & sanction the US for breaking EU-US umbrella agreement".

In reaction, the European Commission issued an official statement, stating that it was "aware" of the executive order and that the US Privacy Act has "never offered data protection rights to Europeans". The European Commission is closely following on the matter. According to PC World, a spokesperson stated: "We will continue to monitor the implementation of both instruments and are following closely any changes in the U.S. that might have an effect on European's data protection rights".
Read more:

The White House - Executive Order: Enhancing Public Safety in the Interior of the United States

Wired - New presidential order could wreck US-EU Privacy Shield

PC World - Trump's executive order won't destroy Privacy Shield, says EU

Meitu defends its selfie app data tracking

Anime selfie app Meitu is responding to reports that it is collecting and sending back to China more data from users' phones than is necessary. According to PC Mag, the company acknowledged that it collects data such as MAC address/IMEI number, IP address, SIM card country code, GPS and network location, and phone carrier info. It says this is within Apple's iOS developer guidelines and terms and similar to those on popular photo-editing apps for Android users. It further stated that because the company is headquartered in China, it was necessary to include the data collection code in the app to circumvent the country's blockage of tracking services from the app stores.

Read more:

PC Mag - Meitu defends selfie app data tracking

Ars Technica - Megaviral Meitu “beauty” app's data grab is anything but skin-deep

Swiss-US Privacy Shield for the transfer of data

On 11 January 2017, the Swiss Federal Council announced the establishment of a new framework for transferring personal data from Switzerland to the United States: the Swiss-US Privacy Shield. The Swiss-US Privacy Shield replaces the so-called Safe Harbor framework between Switzerland. With the establishment of the Privacy Shield, Switzerland will apply similar standards for data exports to the US as the European Union (EU), which set up a comparable system, the EU-US Privacy Shield.

Read more:

Swiss-US Privacy Shield: new framework for the transfer of data to the USA

Undercover investigation by UK consumer group reveals massive sharing of personal data

A new undercover investigation by UK consumer
watchdog group "Which?" has uncovered that personal and financial information is being bought and sold "on a huge scale". The group posed as a dodgy pension advice company looking to operate a common scam and approached fourteen list brokers gaining easy access to over a half a million names, telephone numbers, and pension details. According to the group, many companies were operating illegally and only four companies contacted carried out any kind of due diligence or background checks on the company they posed as. Some of the information sold had not been given consent to be so by consumers.

Read more:

The Independent - Which? undercover investigation reveals personal data being sold on a large scale

Which? - How your data could end up in the hands of scammers

Future events

SciTech's 10th Annual pre-RSA Face-To-Face ISC Meeting

SciTech's 10th Annual pre-RSA Face-To-Face ISC Meeting will be held on February 12-13, 2017 at Jones Day LLP in San Francisco. Topics of discussion will include: IoT Cyber Security & Privacy, The Tech General Counsel: Changing Goals/Changing Roles and more! View agenda and register now.

SAVE THE DATE!

2017 Internet of Things National Institute

May 10-11, 2017 - Washington, DC

Mark your calendars now to attend this conference to learn about this fast emerging, most transformative, and potentiailly most disruptive technology development in years!