I GOT ROBBED! HOW NYS AND THE US SHOULD PROTECT YOUR DATA ONLINE

By Clyde Vanel, NYS Assemblyman, Chair, Subcommittee on Internet & New Technologies

"HELP, I GOT ROBBED!" I felt like screaming that line on Tuesday night, when I first discovered that I was a victim of a scam wire scheme. For nearly a year, I have been working on a new business venture. I am in the process of manufacturing and marketing my first product to the general public.

For the past few weeks, I have been working with the overseas manufacturer on my first large-scale production. Once I approved the samples and packaging design, it was time for production. I was to pay 30% on order and the remainder once they completed the order. I communicate with the manufacturer primarily on electronic mail. A few weeks ago, I sent the deposit to them via international bank wire. A few weeks later, I receive an email, from a similar sounding email, stating that I should send the remainder of the payment to a different bank account in the same country due to high taxes and fees.

Excited to get the product to the States so that I can start selling, I rushed to the bank to send the wire. On the next business day, I sent an email to the manufacturer to confirm their receipt of the funds. They told me that they had not received the money. "Certainly, they were confused" I thought. When I sent them the wire information, they told me it was not their account. They told me that I sent seventy percent of the payment, thousands of dollars, to a scammer.

After roaring, sending angry emails and properly reporting the incident to the bank and the authorities, I thought about the United States and New York State data protection regime. Interestingly by May of 2018, the manufacturing company will have a higher duty of care to protect European nationals' personal data and may be exposed to more liability for such breaches of European nationals' personal information.

EQUIFAX DATA BREACH

Last summer, cybercriminals misappropriated at least 143 million American consumers sensitive personal information at Equifax, one of the nation's three major credit reporting agencies. According to Equifax, the breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. And they grabbed personal information of people in the UK and Canada too. Equifax did not disclose the breach until more than two months after the breach.

US AND NYS CURRENT DATA PROTECTION

In the US, there is no single, comprehensive national law regulating the collection and use of personal data. Instead, we have a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. Additionally, there are many governmental agency guidelines and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices". These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.

There are already a panoply of federal privacy-related laws that regulate the collection and use of personal data. Some apply to particular categories of information, such as financial or health information, or electronic communications. Others apply to activities that use personal information, such as telemarketing and commercial e-mail. In addition, there are broad consumer protection laws that are not privacy laws per se, but have been used to prohibit unfair or deceptive practices involving the disclosure of and security procedures for protecting, personal information.

Some of the regulations include: the Federal Trade Commission Act (FTC Act), the Financial Services Modernization Act (Gramm-Leach-Bliley Act), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act, the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), the Electronic Communications Privacy Act (Computer Fraud and Abuse Act), State data and privacy laws.

Our country and New York's data and information regulation regime is inadequate to protect Americans and New Yorkers sensitive information online.

EUROPEAN DATA PROTECTION (GDPR)

On April 27, 2016, the European Parliament, the Council of the European Union (EU) and the European Commission passed the General Data Protection Regulation (GDPR). The regulation is intended to strengthen and unify data protection for all individuals within the EU. It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the European member countries. The regulation becomes enforceable in the EU on May 25, 2018. It extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, therefore making it easier for US and NYS companies to comply with the regulations. However, the regulations come at the cost of a strict data protection compliance regime with severe penalties of up to 4% of worldwide turnover. The GDPR also brings a new set of "digital rights" for EU citizens in an age when the economic value of personal data is increasing in the digital economy.

THE GDPR

The regulation applies if the data controller (an organization that collects data from EU residents) or processor (an organization that processes data on behalf of data controller, cloud service providers) or the data subject (person) is based in the EU. Furthermore, the regulation also applies to organizations based outside the EU if they collect or process personal data of EU residents. According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

THE GDPR EXPANDS DATA RESPONSIBILITY AND ACCOUNTABILITY

The EU notice requirements remain and are expanded. They must include the retention time for personal data and contact information for data controller and data protection officer must be provided. Automated individual decision-making, including profiling is contestable. Citizens have rights to question and fight significant decisions that affect them that have been made on a solely algorithmic basis.

In order to be able to demonstrate compliance with the GDPR, the data controller should implement measures which meet the principles of data protection by design and data protection by default. Privacy by Design and by Default require that data protection measures are designed into the development of business processes for products and services. Such measures include pseudonymising personal data, by

the controller, as soon as possible. It is the responsibility and liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller.

Data Protection Impact Assessments must be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities is required for high risks. Data Protection Officers are to ensure compliance within organizations.

They have to be appointed:

for all public authorities, except for courts acting in their judicial capacity;

if the core activities of the controller or the processor consist of:

processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;

processing on a large scale of special categories of data and personal data relating to criminal convictions and offences .

Lawful Basis For Processing:

Data can only be processed if there is at least one lawful basis to do so.

The lawful bases for processing data are:

the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

processing is necessary for compliance with a legal obligation to which the controller is subject.

processing is necessary in order to protect the vital interests of the data subject or of another natural person.

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Consent

Where consent is used as the lawful basis for processing, consent must be explicit for data collected and the purposes data is used for. Consent for children under the age of 16, must be given by the child's

parent or custodian, and verifiable. Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn.

Data Protection Officer (DPO)

Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, or where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation.

The DPO is similar but not the same as a Compliance Officer as they are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data. The skill set required stretches beyond understanding legal compliance with data protection laws and regulations.

The appointment of a DPO within a large organization will be a challenge for the Board as well as for the individual concerned. There are myriad governance and human factor issues that organizations and companies will need to address given the scope and nature of the appointment. In addition, the post holder will need to create their own support team and will also be responsible for their own continuing professional development as they need to be independent of the organization that employs them, effectively as a "mini-regulator".

Pseudonymisation

The GDPR refers to pseudonymisation as a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information. An example of pseudonymisation is encryption, which renders the original data unintelligible and the process cannot be reversed without access to the correct decryption key. The GDPR requires that this additional information (such as the decryption key) be kept separately from the pseudonymised data. Pseudonymisation is recommended to reduce the risks to the concerned data subjects and also help controllers and processors to meet their data-protection obligations.

Although the GDPR encourages the use of pseudonymisation to "reduce risks to the data subjects," pseudonymised data is still considered personal data and therefore remains covered by the GDPR.

Data breaches

Under the GDPR, the Data Controller will be under a legal obligation to notify the Supervisory Authority without undue delay. The reporting of a data breach is not subject to any de minimis standard and must be reported to the Supervisory Authority within 72 hours after having become aware of the data breach. Individuals must be notified if adverse impact is determined. In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach. However, the notice to data subjects is not required if the data controller has implemented appropriate technical and organizational protection measures that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.

Sanctions

The following sanctions can be imposed:

a warning in writing in cases of first and non-intentional non-compliance,

regular periodic data protection audits,

a fine up to 10000000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, where there has been an infringement of certain provisions.

a fine up to 20000000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, where there has been an infringement of certain provisions.

Right of access

The Right of Access is a data subject right. This gives citizens the right to get access to their personal data and information about how these personal data are being processed. A Data Controller must provide, upon request, an overview of the categories of data that are being processed as well as a copy of the actual data. Furthermore, the Data Controller must inform the data subject on details about the processing such as; what the purposes are of the processing, with whom the data is shared and how it acquired the data.

Right to erasure

Under the GDPR, the data subject has the right to request erasure of personal data related to them on any one of a number of grounds including non-compliance with lawfulness that includes a case where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Data portability

A person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. Data that has been sufficiently anonymised is excluded, but data that has only been de-identified but remains possible to link to the

individual in question, such as by him or her providing the relevant identifier, is not. Both data that has been 'provided' by the data subject, and data that has been 'observed' — such as about their behavior — is within scope. In addition, the data must be provided by the controller in a structured and commonly used Open standard electronic format.

Data protection by Design and by Default

Data protection by Design and by Default requires that data protection is designed into the development of business processes for products and services. This requires that privacy settings must be set at a high level by default and that technical and procedural measures should be taken care by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. Controllers should also implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.

A by ENISA (the European Union Agency for Network and Information Security) elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. The report specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys.

WE SHOULD STUDY SUCH AN APPROACH TO DATA REGULATIONS

Under EU's GDPR, US and New York companies that control or process EU residents' personal data must comply with the provisions of the law. In the United States and in New York we do not provide such data protection. In fact, if we had such data regulations, I may be better able to address the wire scam.

I recently introduced a bill, A9013, which would create a commission to study our cybersecurity and study the GDPR. In this economic environment, data is invaluable and its value will increase. New Yorkers' personal sensitive data is vulnerable. We must have a data regulation regime that properly protects your information.