Top Data Privacy Issues To Scare You In 2016 - InformationWeek

Pablo Valerio
Commentary

In 2016 issues regarding privacy, whether in personal or business data, are going to dominate headlines and change the way people interact with technology and the companies that provide it. From encryption to drones, to personal information, here's what to watch in the next 12 months.

When it comes to guarding data, whether it's your personal email or the company's balance sheet, nothing is easy anymore. In fact, privacy is one area that's about to have a serious debate in 2016, as individuals, companies, and governments clash over what can or can't be accessed.

A great example of this happening between two close Western partners: The US and European Union.

To start 2016, most companies, primarily US-based Internet providers with users in Europe, are operating in a legal limbo, since there is no current framework for the collection and storage of personal information across the Atlantic. That is because just three months ago the European Court of Justice (ECJ), struck down the 27-year-old "Safe Harbor" agreement between the EU and the US.

Users of popular services such as Gmail, Instagram, and Facebook could be seriously affected if a new agreement is not reached soon, since any cloud provider will be forced to store all data locally in every country. Is that only personal email or social media? What about company data that flows across borders?

With that as a backdrop, I want to address three specific issues that individuals, IT managers, and CIOs should watch in the next 12 months: Encryption, drones, and a new privacy directive in Europe. These are important and shouldn't be forgotten during 2016.

(Image: D3Damon/iStockphoto)

War On Encryption

The so-called crypto-wars began in the 1970s when the US government attempted to classify encryption as munitions.

Until 1996, the US government considered anything stronger than 40-bit encryption illegal to export. Before 1991, the government and large companies were the only real users of encryption technology. But then programmer Philip Zimmermann released free software called Pretty Good Privacy (PGP), which can encode ordinary email. When PGP appeared in other countries, the Department of Justice launched a three-year criminal investigation of Zimmermann.

During the past two years law enforcement agencies on both sides of the Atlantic have been voicing concerns about the use of "Zero-Knowledge" approach to encryption. Zero-Knowledge services allow users to encrypt data and communications with their own generated keys that service providers can't unlock. Big tech companies such as Apple and Google have started letting users encrypt their mobile devices, on both iOS and Android, with private encryption keys.

Apple and Google argue that they won't be able to unlock the device's data without the user's cooperation. While the Obama administration said earlier this year that they won't seek a ban on encryption, the recent terrorist attacks in Paris and San Bernardino, Calif., have triggered renewed efforts to require that Internet companies and service providers make it possible to break encryption if served with a court order.

At the heart of the debate is the question about how the government deals with the fact that communication data is increasingly being encrypted.

In 2014, the US toyed with the idea of a key escrow, something that required all providers to have a "spare key" with a trusted third party that can be requested by the government. Technology companies strongly refused to consider the idea, arguing that could create an administrative nightmare and users will reject it.

Now the UK is preparing a set of new laws that actually ban Zero-Knowledge encryption, and British Prime Minister David Cameron said after the Paris terrorist attacks that there should be no "means of communication" which "we cannot read." Australia already went so far as trying to ban research on cryptography.

But most technology and security experts have been warning about the risks of "backdoors" for law enforcement, arguing that their existence will be eventually exploited by criminals to access critical data. Many services including the BlackPhone and Silent Circle will continue to offer full Zero-Knowledge encryption on their servers located in countries such as Switzerland.

Surveillance and Drones

The US Federal Aviation Administration started registration of "Small Unmanned Aircraft -- better known as drones -- on Dec. 21. The new rules establish that devices weighing "more than 0.55 pounds (250 grams) and less than 55 pounds (approximately 25 kilograms), including payloads such as on-board cameras, must be registered."

Existing drones that were operating before the rule need to be registered by Feb. 19, and new ones need to be registered before the first flight. So, if Santa got you a new drone for Christmas, make sure you tell the government before playing with it outside. Registration is free until Jan. 20, and the FAA will collect a one-time fee of $5 afterwards.

[Read more about the FAA's proposed drone regulations.]

Personal drones can't fly over 400 feet altitude, need to be visible by the operator, can't be flown near airports, groups of people, stadiums, sporting events, or any area where emergency agencies are operating.

But the real battle is now up for states and towns to regulate their use in their communities. While people could fly their drones in their back yard, they could be subject to serious fines if the device flies over to their neighbor's yard or if it uses a camera to monitor his or her activities. In Louisiana, for example, it's illegal to use a drone to monitor a person or property without consent. Offenders face a fine of up to $500 and six months in jail.

Cities such as New York are already looking for a complete ban on the use of those devices, including drones for commercial purposes and law enforcement.

New European Union Privacy Directive

Recently, the European Parliament approved the new EU Privacy Directive, the most comprehensive set of rules to protect user privacy on the continent. As with the Safe Harbor rules, the new Directive limits the amount of data that companies can collect, store, and process. It also and requires explicit user consent to share data with third parties, even if data is technically "aggregated" and "anonymized."

It also raises the age of data consent to 16. Users younger than that will be required to get parental permission to share information about themselves. This effectively will require that companies such as Facebook will require parental consent to open and keep accounts for youngsters. Previously the age of consent was 13.

Technology experts already call the new rules "restricting" but there are some benefits. For instance, it's a single framework rather than separate and sometimes slightly different rules previously used by the European Union's 28 member countries. This had been a major headache for firms doing business across Europe.

Companies found breaking the rules could face fines up to 5% of their global revenue, which is a staggering amount of money for companies such as Google or Facebook.

The Directive needs to be approved by the European Commission and the European Council before it becomes European Law. The approval is usually a rubber-stamp procedure.

Pablo Valerio has been in the IT industry for 25+ years, mostly working for American companies in Europe. Over the years he has developed channels, established operations, and served as European general manager for several companies. While primarily based in Spain, he has ... View Full Bio