PARABLU

Regulation: Regulate or perish, Understanding Data Regulation Today

If you've even been following the news, even casually, you would have noticed that a good part of 2018 was spent discussing data privacy or the lack of it thereof. What is now well established is that an average individual knowingly or unknowingly shares a substantial amount of their data with online services. The fight for individual privacy dates back to a Harvard Law Review article authored in 1890 by Brandeis and Warren. From the time of the "right to be let alone" back in 1890 to "the right to be forgotten" which became part of mainstream consciousness in 2014, the case for data privacy has gained considerable momentum. Now, organizations are being increasingly held accountable for protection of data they store of their employees and customer. The onus of protecting private data has undergone a shift from being an individual's responsibility to being one of the organization's responsibility.

Possibly the very first attempt at regulation in modern times was the Electronic Communications Privacy Act of 1986 which Ronald Reagan helped pass in the US. Since then we've seen several regulations come into effect such as **HIPAA** (Health Insurance Portability and Accountability Act) in 1996 and **SoX** (Sarbanes-Oxley) in 2002. Both of these dealt with access to local data, emphasized the importance of maintaining back-ups of critical data and were instrumental in pushing the envelope when it comes to data regulation.

PARABLU

In 2004, California passed ground breaking legislation making them the first state in the US which required online services to post a "**privacy policy**" on their websites to inform consumers how the provider handled personal information they were collecting. Then came the **HITECH** (Health Information Technology for Economic and Clinical Health Act) in 2009, which not only expanded the scope of privacy and security protections available under HIPAA, but was also more stringent in terms of liabilities for non-compliance. More recently, the **NYDFC** CyberSecurity regulation came into effect. These are a new set of regulations from the NY Department of Financial Services that were released in Feb, 2017. This regulation requires any banks, insurance companies and other financial institutions in New York or having branches in New York State to protect customer data due to the increased sophistication of attacks by cyber criminals.

Protecting private data has undergone a shift from being an individual's responsibility to being one of the organization's responsibility.

Most regulations though ask for the same basic compliance of organizations:

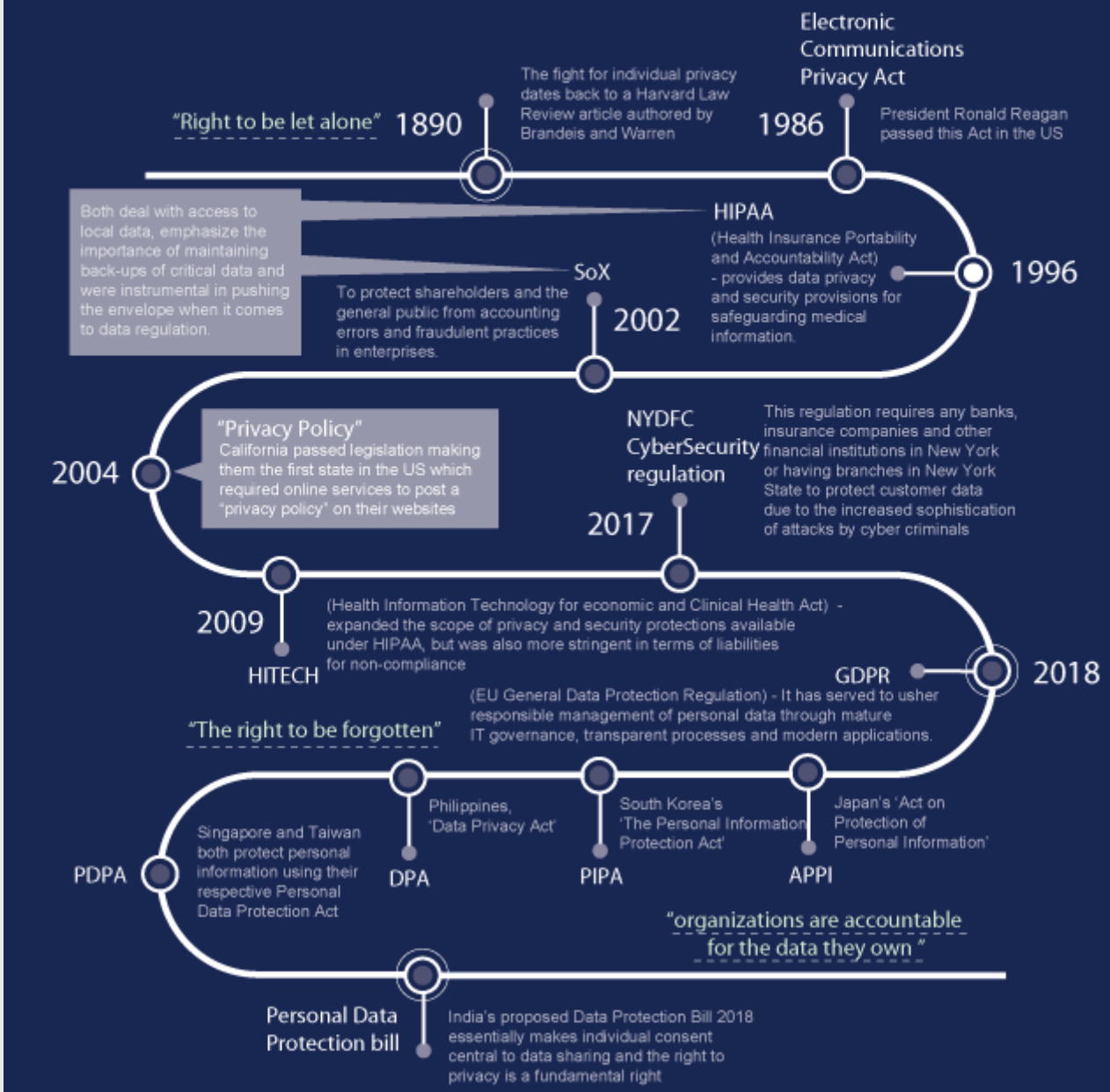
- Know what you have
- Manage access to what you – and make sure it doesn't fall in the wrong hands
- Protect / Save what you have – so you don't lose it in case of a disaster
- Prove that you have processes that are doing the above on a regular basis

The only thing that is a constant is that regulations are increasingly making organizations more and more accountable for the data they own – and that trend is unlikely to change, at least in our lifetimes.

The most recent in the series of regulations that have come into enforcement is the GDPR. GDPR is ground breaking in several ways, not least of which is the fact that the penalties for non-compliance are steep – steep enough to get the attention of almost all businesses worldwide.

PARABLU

Then and now : Key Regulations that shaped the history of data protection



For one thing, the GDPR tends to place citizen rights at a higher plane than the Executive Branch's right to collect information on its citizens. There is also a better attempt to define what 'personal data' is. This may not be as straightforward as simply saying let me look for PII – like Social Security #s or Aadhaar #s or PAN #s and remove them. Any data that singly OR in conjunction with other data to identify an individual. So, you need to be mindful of seemingly disparate pieces of information about a person which individually won't uniquely identify them – but when put together can uniquely identify a person. GDPR also has strict rules about notification and even going public within 72 hours of a breach. Also, as I mentioned earlier, GDPR has teeth, more so than previous regulations. It can hurt organizations where it matters most – penalties can be as high as 4% of annual revenues, not to mention the negative public relations fallout.

GDPR penalties can be as high as 4% of annual revenues

The GDPR came into effect May of 2018, in an effort to protect the data of anyone residing in EU, and is designed to come into more complete effect during 2019. It has served to usher responsible management of personal data through mature IT governance, transparent processes and modern applications. Several nations have privacy protection laws already and many are following the lead of GDPR and are amending their laws to match the same rigor GDPR brings. **Australia has the Privacy Act** which came into effect in 2014. Japan has the **Act on the Protection of Personal Information (APPI)**, South Korea has the **Personal Information Protection Act (PIPA)**, Philippines, the **Data Privacy Act (DPA)**, while Singapore and Taiwan both protect personal information using their respective **Personal Data Protection Act (PDPA)**.

Closer home, India's **Information Technology ACT of 2000**, doesn't come close to the type of protection GDPR affords, but India has already drafted legislation in the form of the Personal Data Protection bill during 2018 and it probably won't be long before India also has its own GDPR equivalent.

Like to know more about regulation, especially GDPR? How will GDPR affect your business? And how to comply with GDPR? Watch this space for more!