https://www.welivesecurity.com/2018/01/18/trends-2018-personal-data-new-age-technology-legislation/

BY TONY ANSCOMBE POSTED 18 JAN 2018 - 11:58AM

Privacy is, or should be, a fundamental human right. Nowadays, the understanding of what the term privacy means for the end user inclines towards data privacy or information privacy. This deviation makes maintaining the desired data-neutral position for the end user increasingly complex. On one hand, there are extremely technology-driven privacy enthusiasts who cultivate zero digital footprint anywhere, on the other – in real life, the vast majority of end users leave a footprint everywhere; giving cybercriminals a web-scape full of sensitive data that looks like a sandy beach on a busy day.

Data is driving the next revolution in technology and feeding the vast artificial intelligence (AI) systems being built. The question is: when any sensitive data enters one of the systems, how many machine-driven decision-making processes will be able to enforce the right to erasure and the right to be forgotten and will the companies collecting this data understand where and how it is being used by their AI systems?

While the majority of end users understand that they are giving their data to social networks or to companies through forms and applications, there are many other providers and services whose data-collecting may not be so transparent.

Free software and services

As consumers expect to enjoy software at no cost, or very low cost, some vendors have taken the decision to enter the data-collection and data-sharing business. Providers of free software only have a few methods by which to monetize their products and the least intrusive, at least from the perspective of what the end user actually sees, could be the collection and sale of data to third parties.

In the past year we have seen trusted security vendors deciding to offer free anti-virus products. While they may not have openly declared their intentions as to how the monetization of their new, free products will work, we can expect to see some of them use indirect monetization methods such as data collection.

The trend of offering of free antimalware products, and the likely monetization of them through indirect means, seems to have accelerated after Microsoft began offering Windows Defender Antivirus as a free default option. Naturally, as a percentage of users shift to the Microsoft by default option, there is less opportunity for existing vendors to sell software, hence the appetite for alternate monetization via offering their own free software rather than direct competition.

The free or low-cost cybersecurity software will continue trending over the next year. This will increase risks connected with data privacy, as free software usually lacks traditional monetization methods, and instead, introduces complex disclosure statements that are in part designed to obscure intent as to what data is being collected and whether it can be sold. This is evidenced by the many companies offering lengthy and unreadable privacy policies that are comprehensible only to lawyers.

Thus, with any free product it is important that a user understands how the company is making money: for example a mobile game may show adverts, or upsell levels of the game. If it is not obvious how the company makes money, then it is highly likely your data and privacy are the method of monetization.

Internet of Things

While free products and apps are all-knowing about our online habits, the adoption of Internet of Things (IoT) devices means that even more sensitive data is now available for collection and exploitation.

As you drive home from work, your phone is transmitting traffic conditions to share with other drivers, hopefully allowing you to make intelligent detours or driving decisions to get you home earlier. The connected thermostat at home is communicating with your phone, relaying your location and the time of day. Currently, you are homeward bound. As you enter the suburban street where you live, the garage door opens automatically, using your proximity to make a decision. The lights come on and your current choice of music transfers from the car to your home automatically. IoT devices are designed to work together, simplifying our existence.

And every device can tell a story via the data it collects. Combining those various data streams, any attacker will be able to paint a full picture of your life: where we work, where we eat, when we go to the gym, what cinema we visit, where we shop and so on. The combination of this data and advances in machine learning and artificial intelligence could mean that we start becoming puppets of technology as it increasingly makes decisions for all of us.

Analysts at Gartner predict that in 2018 there will be 11.2bn connected devices in the world, rising to 20.4bn by 2020. The rise of the machines is coming, beware! Every time a device asks to be connected we need to educate the end user to read the privacy policy and to make informed decisions about whether or not to accept the data collection terms as set out in the privacy policy.

Legislation

Starting in May 2018, the European Commission's General Data Protection Regulation, a directive that gives citizens more power over how their information is processed and used, comes into effect. The legislation affects any company processing or collecting the data of a European Union citizen, regardless of where the company is based.

Non-compliance could result in large fines, but there is no clear answer as to how these fines will be imposed on companies outside of the EU. The Commission may feel that it needs to make an example of a company located outside of its territorial borders, and, potentially, very soon after the May 25th implementation date. Without such an example of enforcement many international companies may take the risk of non-compliance, so we might see the European Commission step up and take action in 2018.

Privacy in the US took a backward step in 2017 when the new administration repealed pending legislation that restricted internet service providers (ISPs) from collecting customer data without permission. While some ISPs have made a voluntary pledge not to allow third-party marketing, that does not mean they will not use such data for their own commercial gain.

The depth of data collected from our online habits could easily allow profiles to be constructed, showing what may be considered extremely personal interests, drawing on information that we don't realize someone is collecting.

Customer profiles could become the target of hackers and we have seen individual data breaches of data sites, stores and others sites. Stealing data that is generated by watching everything we do online could be the ultimate prize to a cybercriminal, offering the opportunity to blackmail users based on their online habits.

The ability to manipulate huge amounts of data as described above and then to use it for something meaningful is a relatively new option for many software and service providers, as the associated storage and processing costs have dropped massively. The 'big data' ecosystem now means that many more companies have the ability to collect, correlate and sell their data.

The ease with which companies can collect data and sell it, our willingness to accept the default settings, and our avoidance of actually reading a privacy policy, means that our identity, way of life and personal data are becoming a corporate asset.

I hope that 2018 brings about greater user awareness, but realistically I suspect it will see greater amounts of data collected with little awareness on the part of the user. With every device that gets connected without informed decision or choice, our privacy is eroded further, until at some point privacy will be something that only our ancestors enjoyed.

https://www.welivesecurity.com/author/tanscombe/

TONY ANSCOMBE

GLOBAL SECURITY EVANGELIST & INDUSTRY AMBASSADOR

Education: Cobol and Fortran programming, it was a long time ago.