# How to secure privacy in the IoT

To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

IoT has proven extremely efficient in its ability to churn out piles of data. Where it stands to improve, and which will be an area of focus in 2017, is in its analytic capabilities. Learning how to derive meaning from the ones and zeroes as they pour in and, more importantly, act on that knowledge while it is still relevant, will be the challenge many businesses begin to tackle in 2017.

APIs are not a new invention. We use them daily to book flights, order products and make secure payments online. Yet, compatibility issues have historically made it difficult for businesses to integrate their software. Additionally, companies have historically only exposed part of their technology through externally-facing API's and never provided access to the rest, restricting it to a single "in-door" that only allowed the most basic in/out.

Internet of Things, or IoT, has changed the frequency with which we actually interact with machines. Last year, there were an estimated 6 billion IoT devices in use, and it's not only consumers using them. Everyone, from organizations to governments are looking at IoT to streamline processes and improve productivity in newer ways. Their use is actually expected to triple in the next five years.

However, the benefits IoT offers, and the way it could reshape the economies are undeniable. Quite possibly we have not even begun to scratch the surface. TfL's use of IoT comes from the fact that London is soon going to be a 10 million strong city, and there is little space to grow. You might imagine IoT managing shifts of commuters travelling at specific times to spread the load more evenly. As Douglas Coupland said this week 'The 9â⍰⍰5 is barbaric'

Most healthcare providers don't have the resources or expertise to execute an IoT strategy on their own?â⍰⍰?especially when it comes to security and privacy issues. Smart partnerships with the right service providers help to fill the gaps and provide added benefits in greater knowledge and due diligence. Businesses need to recognise that IoT has resulted in an increased emphasis on collaboration and the forging of partnerships to maintain a competitive edge. "If reports are to be believed, there will be 1 trillion connected devices worldwide and 100 things per person by 2035," says Mustapha Zaouini, Founder of Fliptin ?â⍰⍰?global provider of ready-made, scalable and easy-to-integrate backend solutions. "Businesses need the ability to handle the complexity, security, scalability and integration of IoT projects?â⍰⍰?not to mention on-going data analysis and usability.

Technology is a bridge that connects a business to the global market. Fast growing use of emerging technologies has created a threat to human privacy. Today organizations have no other choice than being dependent on technical solutions for saving its security. Now it has become very hard to make a proper balance between human privacy and organizational security. Managers want to keep a detailed information about its investment in resources and staff so productivity fetched could be calculated correctly hence, employee monitoring has become must now. Automation has been introduced in order to help to raise productivity stats of any organization not to hurt employee personal life flexibility. And, here integrity must be followed strictly.

Marketers, if you think the Internet of Things is just about controlling your central heating with your phone, you need to think again. The Internet of Things (IoT) will completely change your marketing department. In fact, it's already doing so for many businesses. So, it's worth getting up to speed right now so you can stay ahead of the curve.

There are bots all over the internet that attempt to crack passwords through brute forcing. This is an automated attack that attempts to crack a password by testing every possible combination. This is why having a long and secure password is incredibly important. A short password can be cracked in seconds, whereas a long password may require many more attempts.

You may have recently seen your Facebook trending news telling you how Republicans sold out your privacy to Internet Service Providers (ISPs)â⍰¦you know, on the right just above the ads for the shoes you were browsing yesterday on Amazon. A quick probe of this topic on Google, and you'll find that the issue has become surprisingly partisan, and opinions come down on both sides.

I've been mostly on an airplane the past 4 months, traveling to conferences and IoT ecosystems, meeting amazing founders who will make up the next Techstars IoT class. In fact, I'm just back from Collision in New Orleans which stacks high on my list?â⍰⍰?dense with founders and VCs while thin on service providers and big co logos.

With that guiding principle, ForHumanity presses forward to examine the key risks associated with AI and Automation, Safety & Control, Ethics, Bias, Privacy and Security. We will try to identify the risks and solutions to those risks with the aim to provide each member of society the best possible outcome along the way. There may be times that ForHumanity comes across as negative or opposed to technology, but in the vast majority of cases that is not true. We are just focused on the associated risks with technology. The only time we will be negative on a technology is when the risks overwhelm the reward.

While this is still an emerging technology, facial recognition is a new and exciting tool that has yet to be perfected, paving the way for even more innovations. As this tool advances however, the concern for privacy must remain at the forefront of development, as ethics play an enormous role in the implementation of this breakthrough.

For service providers, YourBlock will offer a secure platform to upload pricing. Merchants and service providers will comply with the new GDPR through the platform. Smart contracts between the consumer and service providers completed on the Blockchain, are immutable, preserving data integrity. YourBlock provides up to date accurate information to service providers, so they may quote with a higher level of accuracy and lower risk factor. YourBlock provides automated compliance with the EU's GDPR data privacy regulations, to simplify and ease transition to compliance for service providers.

It is our sincere hope at YourBlock to facilitate passage to a better world for consumers, merchants and service providers. To provide a universally trusted, secure and efficient platform for the storage of personal data that allows both business and consumer to operate with total transparency. Join us in this digital revolution as we welcome the new era.