International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
*International Conference "*INTELINC 18*", 12th & 13th October 2018*

Apprehension on User's Data Privacy and Data Security in IoT

P. N. Nirmala
Department of Physics, SriMeenakshiGovt Arts College for Women (A), Madurai-2 India.
S.Velmurugan, Capgemini, India
pnnirmala@yahoo.com, velmurugan.sangaiah@gmail.com

Abstract: When more and more devices connected on the internet, the homogeneous network of devices when they are connected via sensors, scanners they turn out to be noticeable in internet. The processed data is communicated over these network might contain user personal data, health data or can even be a financial data.

1. INTRODUCTION

When more and more devices connected on the internet, the homogeneous network of devices when they are connected via sensors, scanners they turn out to be noticeable in internet. The processed data is communicated over these network might contain user personal data, health data or can even be a financial data.

It is important to ensure security and privacy of the user's data[2] when it is transmitted over network. As these homogeneous network of paired devices, the internet of things (IoT), have set up for all users in the network have paved a way to transform the data the way that they wanted to transact or the way that they live in the planet.

Data privacy rules include outdated principles that are found in any other legal framework on data privacy. The arrival of IoT has challenged these traditional principles.

Providing notice to the processed data within the IoT ecosystem may not be feasible, as traditional forms of notice on information practices are difficult to implement in an environment where many sensors/devices at multiple levels are measuring and tracking various data simultaneously. It is not only on processing data it also very important how it is collected before it is getting processed over IoT devices. Hence, it is difficult to give notice in all instances of collection and processing, as it will be very difficult on both the consumers and the IoT stakeholders. The same challenge does exist for providing choice, and written or electronically communicated consent it can be permission or an agreement.

2. USER'S SECURITY AND PRIVACY RISK IN IOT

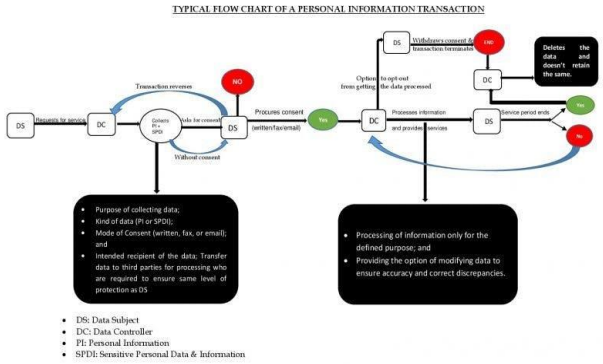
Here's an insight into the impact that IoT may have on laws relating to privacy and data security and the possible solutions in law and industry which will help enable the development of IoT.

IoT devices provide significant benefits to individual consumers across different aspects of their lives. Data and especially personal data (capable of identifying the individual), underpins and delivers most of these benefits. Consequently, the interaction of IoT devices with individuals and their almost unacknowledged but pervasive presence in the daily life and privacy of an individual, would pose ongoing and real-time privacy challenges as well as risks. Before proceeding to explore the implications of the convergent points of the law on privacy and IoT, an understanding of the stakeholders in a personal information transaction would be helpful. One set of stakeholders in an IoT transaction comprise device manufacturers, data platforms, data aggregators or brokers, application developers, social platforms, etc. Their intervention involves extensive access, use and processing of data, resulting in the device operating in an unobtrusive and seamless manner for the user. Another category of stakeholders are the users. In data protection legal frameworks, such stakeholders possess different designations, based on their attributes. There is the 'data subject' (user of the IOT device) who provides the data for availing services and the 'data controller' (IOT device manufacturers/service providers) who controls the data and uses it for providing services/functions rendered through the IOT device. Further, the data may travel through multiple entities present between the data subject and the data controller, who process the data on behalf of the data controller (data processors).

The law on privacy and data security in India in today's electronic age is still at a developmental stage. The Supreme Court has recently recognised the right to privacy in India as a fundamental right under the Constitution. This right also includes the right to informational privacy, which is the individual's right to control the dissemination of his/her data including electronic data and data over the Internet. The Supreme Court of India has also set up a committee (namely B.N. Srikrishna Committee) to frame a legislation on data protection. As a result, any new law on privacy that gets enacted should recognise and accommodate the unique nature of IoT. However, till an omnibus privacy and data protection legislation is put in place, the existing regulatory framework on data privacy and security in India under the Information Technology Act, 2000, merits discussion.

The Information Technology Act, through its Reasonable Security Practices and Procedure Rules in 2011 (Data Privacy Rules) specifies certain requirements for data controllers to follow, while collecting, storing, processing and transmitting personal or sensitive data over the Internet. Under the Data Privacy Rules, the data controller is required to give notice of

the information collected and get the written (or electronically communicated) consent of the user or the data subject, before the data is collected.
The data controller must give the user an option to withdraw consent, change the information in case of a mistake, etc. Further, the collection of information must be limited to the identified purpose for which it is collected, and must be used and disclosed only for the identified purpose (data minimisation). The flow chart below provides a better idea of the flow of information and the regulatory steps involved.



3. RESEARCH DIRECTIONS

Essentially, the Data Privacy Rules incorporate traditional principles found in any other legal framework on data privacy such as notice, choice, consent, and limitations on purpose and collection. The advent of IoT has challenged these traditional principles.
Providing notice to the data subject within the IoT[2] ecosystem may not be feasible, as traditional forms of notice on information practices are difficult to implement in an environment where many sensors/devices at multiple levels are measuring and tracking various data simultaneously. It is difficult to give notice in all instances of collection and processing, as it will be burdensome on both the consumers and the IoT stakeholders. The same challenge exists for following traditional methods of providing choice, and written or electronically communicated consent. Further, most IoT devices do not have a screen or interface where they can communicate notice and obtain consent from the data subject, or the existing interface in the device is not sufficient for such communication.
Data minimisation as a concept, (where companies should limit the data they collect and retain, and dispose it once they no longer need it) may not be realistic for IoT, as it is overtly rigid and may hinder the potential for innovation, in terms of developing and creating more streamlined and refined services within the IoT ecosystem. However, it continues to remain an essential element for the protection of privacy within the IoT ecosystem and cannot be ignored.
The above are just legal touchpoints that demonstrate the gulf between existing law around data privacy and the inherent delivery systems and user interfaces in IoT. The White Paper recently released by the B.N. Srikrishna Committee on data protection laws, has taken the growth of IoT into consideration in contemplating the type of regulation for data protection. However, the onus is not just on the law makers but the IoT industry who need to adopt/reinvent compliant devices, practices and processes that meet current and future data privacy and data protection/security norms.
For instance, IoT industry stakeholders could start with capturing and maintaining user data in an anonymised or de-identified form for services or devices that are not dependent on the identity of an individual. They can adopt a protocol at the device level and user interaction level, to de-identify such data and also ensure that it is not capable of re-identification. Device manufacturers can adopt privacy by design, where privacy and data security measures are incorporated into the design architecture of the device/software. This can ensure that the requirements of data privacy law are incorporated into the device itself and pre-emptively enable data privacy compliance, if not help prevent data security breaches. Of course, a system of frequent security threat and weakness checks and follow-up patches would make this approach more robust.
Notice and consent requirements under the Data Privacy Rules require some form of interface to capture consent and provide policy information on the user's personal information. While high-end IoT device manufactures would most likely have device, application or portal interfaces to meet this requirement, a number of low-end device manufacturers may not (cost being a key deterrent). The requirement could possibly be met through a common portal/network partner (command centre) that allows the user to control the collection and processing of his/her data across various devices and transactions, apart from configuring and controlling device functionality itself.
While there are a number of possible solutions, meeting the challenges that the law poses to IoT and vice versa, requires an effective dialogue between industry and policymakers. Only then would law, technology and society converge in synergistic ways that address industry needs and privacy concerns and thereby fully harness the immense benefits of IoT.

4. RESULTS

Further, the underlying problems of almost all IoT devices are that they do not have UI to communicate either a notice or consent on the data misuse during transactions by a paired IoT device on internet.

5. ACKNOWLEDGMENTS

The work reported in this paper has been partially supported / referred https://yourstory.com

REFERENCES

[1] Data Security and Privacy in the IoT, Elisa Bertino Department of Computer Science Purdue University West Lafayette, IN 47907 bertino@purdue.edu
[2] Privacy in a world of the Internet of Things A Legal and RegulatAory Perspective Research Paper 6
[3] S. K. Bansal. Linux worm targets internet-enabled home appliances to mine cryptocurrencies. http://thehackernews.com/2014/03/ linux-worm-targets-internet-enabled.html, March 2014.
[4] A. Bogdanov and T. Isobe. White-box cryptography revisited: Space-hard ciphers. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015, pages 1058–1069, 2015.

[5] [A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. A large-scale analysis of the security of embedded firmwares. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014., pages 95–110, 2014.
[6] A. Cui, M. Costello, and S. J. Stolfo. When firmware modifications attack: A case study of embedded exploitation. In 20th Annual Network and Distributed System Security Symposium, NDSS 2013, San Diego, California, USA, February 24-27, 2013, 2013.
[7] J. Habibi, A. Panicker, A. Gupta, and E. Bertino. Disarm: Mitigating buffer overflow attacks on embedded devices. In Network and System Security - 9th International Conference, NSS 2015, New York, NY, USA, November 3-5, 2015, Proceedings, pages 112–129, 2015.
[8] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs. Disruptive technologies: Advances that will transform life, business, and the global economy. http://www.mckinsey.com/insights/business_ technology/disruptive_technologies, May 2013. [7] D. Midi, M. Payer, and E. Bertino. nesCheck: Static analysis and dynamic instrumentation for nesC memory safety. 2016. Submitted for publication.
[9] R. V. Nehme, H. Lim, and E. Bertino. FENCE: continuous access control enforcement in dynamic data stream environments. In Third ACM Conference on Data and Application Security and Privacy, CODASPY'13, San Antonio, TX, USA, February 18-20, 2013, pages 243–254, 2013.
[10] K. Rawlinson. Hp study reveals 70 percent of internet of things devices vulnerable to attack. http://www8.hp.com/us/en/hp-news/
[11] Cavoukian, A., & Jonas, J. (2012). Privacy by Design in the Age of Big Data (pp. 1-17). Information and Privacy Commissioner of Ontario, Canada. Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S. (2016).
[12] Privacy and The Internet of Things, Lexis Nexis: Watching Me, Watching You: Surveillance, Privacy and The Media, vol. 21(3), 336-351. Weber, R.H. (2010).
[13] Internet of Things – New Security and privacy challenges, Computer Law & Security Review, vol. 26, 23-30.