HUMAN IMPLANTS AND HACKING

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Melody Musoni | May 20, 2019

When we talk of the risks of the internet of everything, hacking and cybersecurity, what usually comes to mind are the best plausible steps to protect computers, computer systems and computer networks from any unlawful access or interferences. With the emerging medical ICTs, the security of human implants should be part of the conversations on cybersecurity.

Recently, there has been an increase in the use of human implants that are internet enabled and which allows for real-time communications with external computing devices. Human implants include human radio frequency identification (RFID) and implantable medical devices. Human RFID implants are small (approximately 2 mm diameter by 12 mm length) glass capsule-encased passive tags and are typically implanted sub-dermally in the arm or hand.[1] The tags can be functional for more than a decade, though their small size and lack of any internal power source limits performance in terms of memory, processing power and communication range.[2] Implantable medical devices include cardiac defibrillators and pacemakers which are being equipped with features such as data logging and wireless, real-time communications with external computing devices.[3]

Concerns with ICT enabled human implants

Concerns have been raised around the privacy and security issues relating to ICT enabled human implants[4] with IT researchers indicating that human implants can be hacked.[5] Questions have also been raised on whether an attack on an ICT enabled human implant can be considered as vandalism, destruction of property or assault with intention to do grievous bodily harm (Assault GBH). The focus of this article is to give an overview on whether an attack on an ICT enabled human implant can be considered as a cybercrime under South African law.

The cybercrime of hacking human implants

Currently, the Electronic Communications and Transactions Act (**"ECT Act"**) is the law that criminalises cybercrimes.[6] The ECT Act defines data as the electronic representation of information in any form. Under the ECT Act, it is an offence to intentionally access or intercept any data without the authority to do so. Section 86 (2) of ECT Act provides that any person who intentionally and

without authority interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence. This means that if a hacker unlawfully accesses the data contained in an ICT enabled human implant and reprogram the device to malfunction, then such conduct is an offense under the ECT Act.

The ECT Act has been criticised for the limited scope and definitions of cybercrimes as well as a failure to criminalise certain online conduct. This is one of the reasons which has resulted in the introduction of the Cybercrimes Bill.[7] The Cybercrimes Bill criminalises any unlawful and intentional access to data,[8] any unlawful and intentional interception of data including electro-magnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system[9] and any unlawful and intentional interference with a computer data storage medium or computer system.[10] Where a person interrupts the relay of information between the ICT enabled human implant to the doctors remotely monitoring the patient's progress, then such an interference falls within the ambit of a cybercrime under the Cybercrimes Bill. Where a hacker reprograms the human implant such as a pacemaker to result in irregular heart rhythm, then in addition to the charge of cybercrime, the hacker can be held liable on a charge of attempted murder. Where a defibrillator has been reprogrammed by a hacker and causes unnecessary shocks to the patient's heart, then such a hacker can be charged with the crime of attempted murder and assault GBH. Once the Cybercrimes Bill is enacted into a law, any persons who hack into ICT enabled human implants will be committing a cybercrime and be sentenced to fine or imprisonment up to 10 years.[11]

Hacking human implants and privacy

In addition to the criminalisation of the act of hacking into human implants, data protection laws in South Africa also prohibits any unlawful interference with personal information. The Protection of Personal Information Act[12] (POPIA) provides for the conditions that must be complied with when processing personal information. In addition to the conditions for lawful processing of personal information, POPIA prohibits the processing of special personal information, which includes health information.[13] When a hacker intercepts or accesses data contained in an implant, they will also be infringing on a person's privacy and will be in violation of the POPIA conditions for lawful processing of personal information.

Conclusion

With the lack of documented cases in South Africa of hacking of human implants, it remains to be seen how our courts will view such unauthorised access and interference and the forms of punishment that may be imposed on the offenders.

[1] Mark Gasson and Bert-Jaap Koops "Attacking human implants: A new generation of cybercrime" 2013 (5) *Law, Innovation and Technology* 248 at 252.

[2] Mark Gasson and Bert-Jaap Koops "Attacking human implants: A new generation of cybercrime" 2013 (5) *Law, Innovation and Technology* 248 at 252

[3] Mark Gasson and Bert-Jaap Koops "Attacking human implants: A new generation of cybercrime" 2013 (5) *Law, Innovation and Technology* 248 at 254.

[4] Pawel Rotter, Barbara Daskala and Ramon Compano "Passive Human ICT implants: Risks and Possible Solutions" Book Chapter 5 Human ICT Implants: Technical, Legal and Ethical Considerations

Gasson M.N., Kosta E, Bowman, D.M. (Eds) (2012) XXII Asser Press.

[5] https://www.cnbc.com/2018/08/17/security-researchers-say-they-can-hack-medtronic-pacemakers.html accessed 15 May 2019. https://www.reuters.com/article/us-health-heart-pacemaker-cyber/pacemakers-defibrillators-are-potentially-hackable-idUSKCN1G42TB accessed 15 May 2019.

[6] Act 25, of 2002.

[7] Cybercrimes Bill B6B 2017.

[8] Section 2 of the Cybercrimes Bill.

[9] Section 3 of the Cybercrimes Bill.

[10] Section 6 of the Cybercrimes Bill.

[11] Section 19 (2) of the Cybercrimes Bill.

[12] Act 4 of 2013.

[13] Section 26 of Act 4 of 2013.