Rethinking international regulations: Are individuals protected from identity theft?

With over sixty-three per cent of the world's population connected to the internet and the introduction of standards such as EU GDPR (Intersoft Consulting, N.D.) to support users' control and govern their data, data has become a precious asset. The demand for data has grown in cybercrime-as-a-service (CaaS), where the internet facilitates products such as bespoke phishing kits to target victims (Kaur, 2022). These are designed to fool unwary victims into believing they are dealing with genuine parties, ultimately leading to cyber-enabled fraud.

However, the costs to society are far higher, with law enforcement agencies requiring education on protocols to manage investigations and technological development to track perpetrators. The financial cost to the economy is approximately four billion pounds yearly, two and a half times higher than in 2007 (Fraud Advisory Panel, 2007).

In the U.K., social engineering phishing attempts whereby cybercriminals target users to obtain personal data to cause identity theft is trending to a record high in the second quarter of 2022 (Anti-Phishing Working Group, 2022).

Victims of identity theft are not always adequately protected by criminalising identity theft in a national context. The European Convention for Human Rights (Council Of Europe, N.D.) is available as an international regulator to effectively criminalise theft and restore compromised identity to the victim. However, this cannot be done by individual governments and requires collaboration for this cross-border investigation assisting law enforcement (De Schepper et al., 2017).

Nevertheless, Article 8 of ECHR suggests respect for privacy and protect the user, which is helpful despite the protection of human rights relying on the interpretation of member states own legal frameworks (Mammadov, 2021). This raises an inconsistency in practice. EU GDPR has been an effective regulation to overrule national law and investigations.

However, law enforcement authorities face further challenges in providing effective investigations of identity theft due to international regulations of EU GDPR that have created crime incentives unwittingly. Whilst the standard aims to provide greater transparency and governance of data, cybercriminals are exploiting areas. WHOIS listing for internet domain registrations provided by ICANN is no longer public; breaches must be reported in seventy-two hours, and fairness, transparency and lawfulness when data processing means that organisations and identity management are needed, especially with legacy technology that can break GPDR standards.

The collaboration of ICANN and law enforcement would effectively slow the investigation process and increase costs, yet without WHOIS, the internet is not transparent (Ferrante, 2018). Furthermore, EU GDPR does not critically address identity theft crimes, as proposal updates to legislation have not been adopted and does not have a technological approach to assist citizens concerning their data and data is open to vulnerabilities (Jayatilaka, 2020).

Solutions are in consideration to combat identity theft and maintain the integrity of national investigative and international regulations. The Second Additional Protocol to the Budapest Convention on Cybercrime (Polyzoidou, 2021) offers greater

collaboration between authorities and service providers. Mutual legal assistance, data protection, safeguarding of human rights and transborder access to data are included. This offers significant hope, although this would require adoption by all signatory parties and with states considering parallel systems of intenational cybercrime laws, a unified body is needed for success (Zachar, N.D.).

Anti-Phishing Working Group. 2022. *Global Phishing Survey* [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf [Accessed 19 November 2022].

Council of Europe. N.D. *The European Convention on Human Rights* [Online]. Available: https://www.coe.int/en/web/impact-convention-human-rights/how-it-works [Accessed 19 November 2022].

De Schepper, K., Severijns, H. & Verbruggen, F. 2017. Study on criminal law measures to tackle identity fraud and identity theft.

Ferrante, A. J. 2018. The impact of GDPR on WHOIS: Implications for businesses facing cybercrime. *Cyber Security: A Peer-Reviewed Journal,* 2**,** 143-148.

Fraud Advisory Panel. 2007. *Identity Fraud: Do you know the signs?* [Online]. Available: https://www.fraudadvisorypanel.org/wp-content/uploads/2015/05/Identity-Fraud-Do-You-Know-the-Signs-Individuals-A4-Dec07.pdf [Accessed 19 November 2022].

Intersoft Consulting. N.D. . *GDPR* [Online]. Available: https://gdpr-info.eu/ [Accessed 22 January 2022].

Jayatilaka, D. WHAT IS THE EUROPEAN UNION'S DATA THEFT AND DATA FRAUD POLICY AND HOW CAN IT BE IMPROVED? GLOBAL, 2020. 31.

Kaur, D. 2022. *Identity theft are costing the brits £4bn a year.* [Online]. Tech HQ. Available: https://techhq.com/2022/08/identity-theft-is-costing-the-british-4bn-a-year/ [Accessed 19 November 2022].

Mammadov, R. 2021. Is Privacy Still Possible on Social Media? *Available at SSRN 4095320*.