The Complex relationship between fraud and technology - Should we ignore or regulate online platforms?

Author:
Jack Whittaker: PhD Candidate (crim.) at the University of Surrey
j.m.whittaker@surrey.ac.uk

There is little doubt that throughout history there have been many frauds that have been committed with the aid of various technologies. For example, the invention of the printing press by Johannes Gutenberg in 1440 provided with it novel opportunities for offenders to create new means of committing economic fraud by flooding the literature market with the counterfeited works of early publishers. Likewise, the works of Heather Shore in her account of crimes in London from 1720-1930 describes an increase in organised syndicates of "swindlers, coiners and fraudsters" from at least the early 18th century, many of which possessed sophisticated technological know - how. One account provided by a police inspector in 1862 illustrates a particularly salient case whereby an individual called Joseph Jones, his wife Elizabeth Jones, and neighbour William Smith were found to be producing counterfeit florins by electroplating base coins with wires and galvanic batteries, a process which sought to create a silver outer coating on the coin (Shore, 2015, pp. 124). In contemporary society, by contrast, the majority of frauds committed are now perpetrated online in so-called 'cyberspace' (61%) (Ons.gov.uk, 2022).

The growth of online platforms is one such technology that has in the past twenty years provided ample opportunity for fraudsters. In one instance, we have seen the industrialisation of older frauds (Button & Cross, 2017). Academic researchers have uncovered how fraudsters have sought to move away from committing face-to-face frauds in the real world, such as consumer fraud and romance fraud, and that they have sought to perpetrate these crimes online in e-commerce and dating platforms to name but two notable examples. (Treadwell, 2012; Whittaker & Button, 2020; Gillespie, 2017). In addition to this, fraudsters have now sought to create new frauds (Button & Cross, 2017) such as tailor-made 'fraud-as-a-service' products (McGuire, 2017). The opportunity to bulk-buy fake reviews on e-commerce platforms and bank accounts used in laundering the stolen funds of victims on social media websites are two notable examples of this.

A natural question arising from this issue is "should we care that technology is used in the perpetration of fraud?" On the one hand, proponents of the instrumentalism perspective of technology argue that no we shouldn't care. Technology under the instrumentalism perspective is viewed as being neither good nor evil and that it should not be regulated. A notable example of instrumentalism can be attributed to a slogan commonly used by the US gun lobby to oppose the regulation of firearms, that "guns don't kill people, people kill people" (Henigan, 2016). On the other hand, technology can be viewed through the lens of extension theory (See Kepp, 1877; McLuhan, 1964; Brey, 2010) which argues that technology extends human agency by expanding the opportunities of what is capable without the use of technology. Therefore, under the extension theory perspective regulation is necessary because technology amplifies the modern fraudster's capabilities.

Extension theory can also be useful in explaining the growth in fraud victimisation on online platforms. Marshal McLuhan for example in his influential book 'Understanding Media' (1964) argues that in addition to extending capabilities, technology can also result in 'amputations' of various kinds. To use

a simple example of this, one could argue that the development and widespread adoption of guns resulted in a loss of archery skills. In the context of 'cyberspace', users arguably sacrifice their mental faculties like concentration or memory in favour of convenience, the speed at which transactions occur and the opportunity to create new interactions inside of a digital environment. For example, instead of consumers visiting a traditional "bricks and mortars store" to inspect a product and determine that what they are intending to buy actually exists and is of a sufficient quality, consumers that elect to use online retail platforms instead amputate their senses and are more willing to 'trust' that the seller is reputable and not intending to defraud them. Likewise, this is also the case in online dating whereby internet users 'trust' that the person they have met on a dating platform is who they claim to be. Arguably, as well as the increased vulnerability that internet users put themselves at when they are using the services of online platforms, there are also other issues that contribute to victimisation. For example, many online platforms have very little 'know your customer' (KYC) processes. Platforms often purposely open the proverbial floodgates as a means of attracting as many users as possible, particularly when they utilise a freemium business model. In the case of many online dating platforms for example, one can merely sign up for a free account without any formal checking procedures.

Additionally, one can argue that platforms can in fact benefit from fraudsters operating on them. For the purpose of this short article, I have unpacked these into three benefits which are by no means extensive.

1. To inflate user figures. For example, after the Ashley Madison data breach in 2015 it was discovered that nearly every female profile was either fake or dormant as a means of luring men onto the platform (Gallagher, 2015).
2. To generate income. A key component of the online fraud economy is that fraudsters need to spend money to make money. An example of this is how many fraudulent e-commerce websites reinvest their previous victims stolen funds onto search engine advertising campaigns as a means of attracting traffic to their website.
3. To decrease cost. It is simply easier and cheaper for platforms to ignore instances of fraud by not training a well-resourced abuse department.

In summary, this short article has sought to introduce the notion that there is a historical relationship between technology and fraud, that two opposing viewpoints argue whether technology is or is not capable of harm, and lastly that platforms can in fact benefit from fraudsters operating on them parasitically. Given that there is an ongoing tidal wave of online parasitic platform criminality, it is arguably not enough for platforms to continue ignoring the problem of online fraud or for this problem to be moderated haphazardly by abuse algorithms. After all, fraud is an inherently human - centric crime which in most instances relies on communication between the fraudster and their victim, meaning that a trained human is often needed to identify that a fraud is taking place. In the longer term, a suggestion is that 'know your customer' verifications should be a mandated part of any online platform's business model. It is not simply enough for platforms to play whack-a-mole with fraudsters by taking down some fraudulent content only for it to appear again later.

References:

Brey, P. (2010) 'Philosophy of Technology after the empirical turn', Techné: Research in Philosophy and Technology, 14(1), pp. 36–48. doi:10.5840/techne20101416.

Button, M. and Cross, C. (2017) Cyber frauds, scams and their victims. London: Taylor and Francis.

Gallagher, C. (2015) Ashley Madison and the ethics of disclosure! Chuck Gallagher. Available at: https://www.chuckgallagher.com/2015/08/21/ashley-madison-and-the-ethics-of-disclosure/ (Accessed: 27 October 2023).

Gillespie, A. (2017) 'The electronic Spanish prisoner: Romance frauds on the internet', The Journal of Criminal Law, 81(3), pp. 217–231. doi:10.1177/0022018317702803.

Henigan, D.A. (2016) 'guns don't kill people, people kill people': And other myths about guns and gun control. Boston: Beacon Press.

Kapp, E. (1877) Grundlinien einer Philosophie der technik: Zur Entstehungsgeschichte der cultur aus Neunen Gesichtspunkten. Braunschweig: Druck und verlag von George westermann.

McGuire, M. 2018. Into the Web of Profit: Understanding the Growth of the Cybercrime Economy. [online]BromiumInc.Availableat: <https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf> [Accessed 26 March 2021].

McLuhan, M. (1964) Understanding media. McGraw-Hill.

Ons.gov.uk. (2022). Nature of fraud and computer misuse in England and Wales: Year Ending March 2022. Nature of fraud and computer misuse in England and Wales. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/