Understanding 21st century cybercrime for the 'common' victim

Frances P Bernat and **Nicholas Godlove**

argue that it is time to extend the principle of universal jurisdiction to the typical types of cyber-offences

The innovation and ubiquity of computer connective technology has opened a terra nova for illegal activity. People can socialise, game, bank, and manipulate cameras and locks from any location with internet access. In the United States, youth have 'hyper-inter-connectivity' – they are always connected to the internet for information and social contact (Netburn, 2012). Hyper-inter-connectivity connects the younger generation in a worldwide social network: in 2009, about one fourth of the world's population had access to the internet (Lu et al., 2010) and social networking has made worldwide inroads. The new found connectivity allows for the commission of old crimes in new soil: the internet. What this means is that victims are now geographically untied to their victimisers: fraud, theft, or threatening communications have no geographical tether between offender and victim. Notwithstanding its disparate forms, victimisation is commonly called cybercrime.

What is cybercrime?

Cybercrime involves gaining illegal access to or illegal entry into a computer or illegally interfacing with another through the use of a computer. Some cybercrimes are just a new method for committing old offences against property, such as theft and fraud, or crimes against the person, such as harassment and assault. Other cybercrimes are newly created offences, enacted to respond to the computer's ability to be used as a conduit for unacceptable behaviour, such as phishing and hacking. They are typically legislative responses to behaviour that affects government or large corporate interests: advance fee frauds, cyber fraud (through phishing, malware, scamming and hacking), auction frauds, non-delivery and credit-debit card frauds, identify theft, stock market manipulations, investment and pyramid schemes, digital extortion, cyber-terrorism and industrial sabotage, intellectual property infringement, and unauthorized access. Nations and multinational corporations looking to protect themselves against major threats to their computer systems will seek laws to punish and prescript the most serious offences committed via computers. These crimes generally cover large-scale computer misuse, ignoring the use of computers for victimisation of individuals.

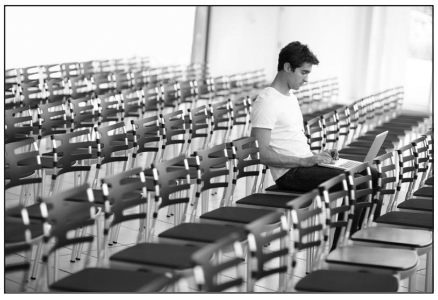
Computer crime in the new century is a moving target. As police and prosecutors shut down one form of online offence, another arises. Established criminal law definitions and applications may not clearly define emergent offending behaviours and nation states may be unable to punish persons for cyber offences that slip between gaps in the law. Additionally, when the offending behaviour travels through cyberspace, the electronic connection may cross international boundaries. This leads to significant jurisdictional problems: where did the crime occur, who will investigate it, where will the crime be prosecuted? Universal jurisdiction, which would enable one nation to exert authority to punish offenders who commit a crime in their nation but who reside outside the nations territorial boundaries, presupposes that a nation should be able to prosecute persons for such major offences as piracy on the high seas or war crimes. The extent to which universal jurisdiction principles apply to cybercrime is still unclear. Finally, cybercrimes are committed behind the veil of anonymity that exists on the internet. The anonymity of the internet may make these crimes difficult to detect for two reasons. Even if cybercrime is detected within a specific jurisdiction that chooses to investigate further, it will be difficult to identify, arrest, and prosecute offenders outside the territorial boundaries of the state.

cybercrimes are committed behind the veil of anonymity that exists on the internet

Problems with helping the 'little guy'

The potential number of victims of cybercrime is nearly limitless; the actual number of victims is unknown. Some estimate that between one quarter to one half of United States businesses have had some form of breach in their computer systems (Fletcher, 2007; Yang and Hoffstadt, 2006). And although the potential impact from cyber victimisation is not inconsequential (estimated annual losses are in the billions or trillions of dollars), companies and nations may not wish to report computer breaches in order to prevent market fluctuations in their stocks or to prevent the public from panicking. Individuals who are not savvy may not even realise they have been hacked. Youth may not want to report personal victimisations to their parents and friends, nor be willing or have the agency to contact police. Thus, we do not really know

10.1080/09627251.2012.721962



the full level of victimisation due to underreporting.

In addition, while much governmental consternation is placed on the protection against infiltration of government computing systems and losses to business, the lion's share of cybercrime victimisation is felt by individuals who have 'small' private financial losses or are targeted for harassment, bullying or stalking. For example, in the United Kingdom, computer crime costs about £1,000 per household each year while in the United States such losses are estimated to be about $4,000 per individual annually (Fletcher, 2007; Tan, 2002). In the United States unless a significant threshold amount or national security concerns are met, federal courts do not have jurisdiction to prosecute the crime. Naturally, the initial legislative response to the emerging field of cyber-activity was to pass laws protecting important national security concerns and the concerns of important financial institutions. But now, will the laws begin to protect the individual? It appears that persons who are most susceptible to cyber property scams and cyber bullying, stalking or harassment offences are persons who regularly use the internet, are young and do not know who to turn to for assistance in abating their victimisation. In some cases, cyber bullying for example, the person may be both an offender and a victim.

Cybercrime exists in a world without and within physical spaces

We presume that the cyber-world is a 'cloud.' But the cloud is based in the real world and real people are being harmed. We have to find a way to 'ground' cyber-activity that harms persons and their computing systems. One of the first areas of legal change has to be in the area of jurisdiction. The primary concerns have been in figuring out which governmental agency has authority to try offenders for the offences, where is the offence to be litigated, whose law applies in enforcement of cybercrime, and what punishments can be imposed? When crimes are committed in a physical location, jurisdiction can be ascertained in accordance with three primary jurisdictional considerations: where did the offence get committed, what is the law within the locus of the offence, and what is the power of the nation (state) to enforce the law that was violated? In traditional cases, it is presumed that the offender and victim were in physical contact with each other. For cybercrimes, this presumption is lost as the offender can be anywhere. The laws of various jurisdictions complicate the matter. Laws in some nations where the computer 'offence' was perpetrated may not recognise the activity as criminal and the nation may not assist with the extradition of their national to another country which considers the activity to be criminal. Traditional laws of property can be inadequate and inappropriate in the cyber-world. Without a physical presence (e.g. looking at a computer virtually or attempting to access another's computer without authorisation but not getting into it) the local laws of many jurisdictions will not proscribe hacking as an illegal act.

Cyber-hyper-vigilance

The internet allows persons to be connected to others anywhere, at any time, in any way. The ubiquity of the internet challenges us to think and respond creatively as computers are used to personally and financially hurt people. Banks and other important institutions have special protections they can use to find and prosecute hackers. It is time to bring these same criminal justice opportunities for redress to more forms of online victimisation. To do this we have to think about cyberspace as having real physical dimensions. While persons may connect to others via the internet cloud, they are physically bound in one place at the time of their computational access and behaviour. Consequently, if the offender and victim are from the same nation, it should not matter if the computer connection travelled through other nations whose laws do not proscribe the offending behaviour; the offender and victim are physically placed in the same nation state and those laws 'physically' fix the parties within the jurisdiction of the nation's courts. If the offender and victim are from different nations, then we need to modify jurisdictional laws so that offenders could be prosecuted in both or either location. Although universal jurisdictional principles aim to punish only serious offences, it could be extended to recognise cyber-crime that harms any person who interfaces with others via computer systems.

In the modern world, computers have become a mainstay for businesses and individuals alike. While cyberspace seems to be a place without a physical presence, there is a real community to it and crime that is committed in it. Computers have a physical presence, servers have a physical presence and people have a physical presence. Such physicality tethers the law to the nation in which the offender and victim reside. ■

Frances P Bernat is Professor and Chair, Texas A and M International University, Emeritus Faculty, Arizona State University. **Nicholas Godlove** is Adjunct Faculty, Arizona State University

References

Fletcher, N. (2007), 'Challenges for regulating financial fraud in cyberspace', *Journal of Financial Crime,* 14, pp. 190-207.

Lu, H., Liang, B. and Taylor, M. (2010), 'A comparative analysis of cybercrimes and governmental law enforcement in China and the United States', *Asian Criminology,* 5, pp.123-135.

Netburn, D. (2012), 'Pew Study: Is the Internet ruining or improving today's youth?', *Los Angeles Times,* February 29.

Tan, H. (2002), 'E-fraud: Current trends and international developments', *Journal of Financial Crime,* 9, pp. 347- 354.

Wong Yang, D and Hoffstadt, B. (2006), 'Countering the cyber-crime threat', *The American Criminal Law Review,* 43, pp. 201-215.