I shop online — recreationally! Internet anonymity and Silk Road enabling drug use in Australia

Amy Phelps [a], Allan Watt [b],[*]

[a] Australia Federal Police, Australia
[b] PICT Macquarie University, Australia

ABSTRACT

Internet technologies are beginning to influence the sale and supply of illicit drugs in Australia. One such technology, an online marketplace known as Silk Road, had dramatically increased in popularity since its worldwide launch in February 2011. This research and paper were completed prior to the Silk Road's founder, Ross Ulbricht being arrested on 2 October 2013 and Silk Road being taken off line. This research paper will consider such factors; as the increasing use of internet by Australians, the popularity of shopping online and the variance in the quality and price of products available on Silk Road to those available in other drug markets. The case study will provide an in-depth look at Silk Road from an Australian perspective and in light of the continuing popularity of illicit drug use in Australia. Though Silk Road is currently off line, 'Bitcoin' has survived and it will only be a matter of time before a substitute for Silk Road emerges.

Crown Copyright © 2014 Published by Elsevier Ltd. All rights reserved.

Introduction

In 1990, when several Australian universities began connecting to the internet[1] for the first time it was anticipated the humble connection would change the face of research in Australia. It was not at that time foreseen the internet would grow to become one of the most relied upon and frequently used tools, not just in Australia but also throughout the world. The exponential growth of the internet has impacted many aspects of Australian culture whilst improvements to technology such as smartphones and tablet devices have allowed Australians to be more connected and more reliant on the internet for everyday use.

Whilst use of the internet is predominantly benign it is inevitable that crime, which often follows opportunity, will shift to exploit the internet and its associated technologies.[2] The term cyber crime has been used to categorise the growing number of crimes involving computers and/or the internet. Cyber crime consists of crimes committed using the internet such as using the internet to sell illegal goods or to distribute Child Abuse Material[3] and of interest to this research is the growth of internet-enabled crime or crime facilitated through communication tools, information sources and recruitment/financial services[4] made possible with internet enabled computers. The internet does not

---

[1] For the purposes of this paper and for ease of reading the word internet will not be capitalised. The internet not capitalised will be used to describe the set of networks that links computers worldwide through a set of communication protocols, as defined in the Oxford English Dictionary.

[2] P Hunton, 'The growing phenomenon of crime and the internet: A cybercrime execution and analysis model' *Computer Law & Security Review*, vol. 25, 2009, p 529.

[3] Global Agenda Council on Organized Crime, *'Organized Crime Enablers'*, World Economic Forum, 2012, p 4.

[4] EUROPOL, 'Internet Facilitated Organised Crime', IOCTA, 2011.

just act as an enabler for child sex exploitation, it contributes to crimes of varying nature including money laundering, human trafficking, drug running and illicit drugs. The internet has become increasingly popular in promoting and facilitating the purchase, supply and manufacture of illicit drugs yet the issue is barely mentioned in cyber crime textbooks[5] and this topic will be explored in this paper.

Literature review

With the growth of cyber crime there has naturally been an increase of attention of law enforcement agencies and criminal enterprises are looking for more and more sophisticated methods for avoiding detection and leading to internet users seeking anonymity. Anonymity, as opposed to being anonymous on your own, refers to 'being indistinguishable in an anonymous set'[6] and allows users to conduct transactions on the internet without being identifiable. Whilst many users want anonymity when accessing the internet much of what we do is monitored and controlled by search engines such as Google and Microsoft who, for example, keep users search data for 18 months.[7] To bypass the strict controls sanctioned by search engines, internet service providers (ISPs), internet filters and law enforcement agencies, some internet users have taken their activity 'underground'. As with real world crime, especially those were the risk is low but the profits high, crime on the internet flourishes in the underbelly of society. This underbelly or underground version of the internet is referred to as the deep web[8] (or deepnet, dark web, invisible web) and is a series of anonymous and virtually untraceable global networks (Goldberg). Within these networks are sites specialising in a wide array of cyber crimes including contract killings, the sale of illicit drugs, computer hacking and malware, money laundering and illegal organ trading (and of course many websites that may choose to be hidden despite the fact they are not conducting illegal activity). The most persistent of crimes being perpetrated in the deep web revolve around Child Abuse Material services and include people trading images, downloading under-age pornography and forums for perpetrators to discuss child sex abuse openly. There are however many other types of sites and one such site previously operating in the deep web, dealing with the sale of illicit drugs and related prohibited paraphernalia was the Silk Road Online marketplace.

The Silk Road Online Anonymous Marketplace (Silk Road) was an anonymous online marketplace that emerged in the deep web in 2011 and was created by a person (or group of people) under the pseudonym 'Dread Pirate Roberts'. Through his arrest it is now known this was, Ross Ulbricht, of San Francisco, California. Described as an 'eBay for drugs'[9] Silk Road was a marketplace for the trading of illicit drugs, drug paraphernalia and other products. Considered to be *sui generis*[10] the website was the only known website at the time of publication openly selling illicit drugs with the same simplicity that Amazon.com sells books. According to the sites administrators, Silk Road was not intentionally created to support illegal trading with creators aiming to build a 'framework for trading partners to come together for mutual gain in a safe and secure way'.[11] The anonymity promised by the site however did entice 'sellers' and 'buyers' looking to trade in illegal products without attracting unwanted attention from law enforcement. Shortly after opening sellers began creating listings for illegal substances including marijuana, MDMA, LSD and cocaine. The sellers, not bound by traditional trading constraints could sell from anywhere in the world with popular listings appearing from the United States, The Netherlands, Germany and Australia.

The site was embedded in the deep web and relied on several mechanisms to ensure total anonymity for sellers and buyers. The first of these are internet anonymisers and in this instance a specific type of anonymiser know as onion routing. Onion routing, a system created to separate the processes of identification and routing through the internet, was first adopted by the Naval Research Laboratory in the United States in 1995.[12] The inventors of onion routing recognised the importance of creating software, which in a world where everything on the internet is monitored could provide users with an opportunity for anonymity. They adapted the onion routing technology into a software program called TOR (The Onion Router) that was released for public use in 2002. Since its inception TOR has grown in popularity, rising from several hundred users to 400,000 in 2011[13] with approximately 3000 volunteers working together[14] to create the anonymous network that is TOR. The program works like a network of virtual tunnels[15] where users around the world volunteer their computer, allowing traffic to bounce through the tunnels so that users cannot be traced to their destination. The identity of a user's IP address is essentially masked so that any website visited or conversations taking place via instant messaging becomes untraceable, or anonymous. TOR, categorised as a type of anonymising software, is not the first or the only software of its type however it has shown to be one of the

[5] N Phair, '*The online environment: a precursor to illicit synthetic drug law enforcement*', NDLERF Research Proposal, 2012, pp. 2.

[6] TORButton FAQ, viewed on 14 September 2012 www.torproject.org/torbutton/torbutton-faq.html.en.

[7] S Mansfield–Devine, 'Google challenged on search privacy', *Network Security*, vol. 2010, 2010, p.2.

[8] E Ormsby, 'The new underbelly', in *The Sydney Morning Herald*, 2012, viewed on 01 June 2012, http://www.smh.com.au/technology/technology-news/the-new-underbelly-20120531-1zktt.html.

[9] M Barratt, 'A trip down the Silk Road', 2011, viewed on 4 February 2012, http://injectingadvice.com/articles/guestwrite/247-monicabarrat.

[10] M Pesce, 'The darknet ages', The Drum Opinion, 2011, viewed on 13 June 2011, http://www.abc.net.au/unleashed/2754260.html.

[11] Silk Road, 'State of the Road Address', 2012, viewed on 5 October 2012, http://silkroadvb5piz3r.onion/index.php/silkroad/home.

[12] P Syverson, 'Practical Vulnerabilities of the TOR Anonymity Network', *Advances in Cyber Security: Technology, Operation and Experiences*, Fordham University Press, Forthcoming edition.

[13] R Henry, '*A Privacy-Preserving Protocol for Gathering Statistics About TOR Users*', 33rd IEEE Symposium on Security and Privacy (Poster Presentation), May 2012.

[14] TOR Metrics Portal, 2012, viewed on 4 February 2012, https://metrics.torproject.org/network.html.

[15] TOR Frequently Asked Questions, 2012, viewed on 4 February 2012, https://www.torproject.org/about/overview.html.en.