Challenging the techno-politics of anonymity

the case of cryptomarket users

Challenging the techno-politics of anonymity: the case of cryptomarket users

Abstract:

Anonymity is treated as a problem of governance that can be subject to technical resolution. We use the example of the darknet to critically examine this approach. We explore the background assumptions that have been made about anonymity as a quality of social life. We conceive of anonymity as a way of engaging and maintaining social relationships in an anonymous mode. We draw on a study of darknet 'cryptomarket' users who mainly use the darknet to buy and sell illicit drugs, discuss drug quality and share information on safe and effective use. We identify the personal satisfaction that comes from interacting anonymously online, the challenges this represents for maintaining trusted interactions and how they are overcome, and the combination of technology and action involved in maintaining anonymity. We argue that attempts to promote de-anonymising norms and technology are based on an erroneous understanding of what anonymity is.

Keywords: cryptomarkets, anonymity, drug use, darknet

Authors:

Dr Angus Bancroft, University of Edinburgh

University of Edinburgh

18 Buccleuch Place, 4.05

Edinburgh EH8 9JS, United Kingdom

Tel: 0131 6506642

@angusbancroft

Peter Scott Reid, independent researcher.

How is anonymity understood and generated in online communities that place a premium on being hidden? The changing salience of anonymity online has recently sparked concerns about, on the one hand, loss of privacy and autonomy in the face of state and corporate surveillance and, on the other, the creation of ungovernable spaces and the facilitation of terrorism and harassment. We argue that, in part, this debate involves some limiting assumptions about what anonymity is and what it means. Public discussions still assume that anonymity is the norm on the internet when it is rare, and it is also assumed that the main threat to it comes from state entities, where it is mostly private companies that assemble de-anonymising technology (Froomkin, 2015). Partly the problem stems from assuming that there always can be a singular, direct connection between real world identity and online persona, and the tendency to reduce the issue to scapegoated technologies and platforms (Scott, 2004). This reduces political questions to technical ones, and obscures how technical and social infrastructures are created in ways that de-anonymise.

We aim to contribute to this debate by critically exploring these assumptions and reflecting on the history of treating anonymity as both productive and suspect, and by drawing on critical digital sociology that exposes the deep technological and social structuring of digital life (Beer & Burrows, 2013; Skeggs & Yuill, 2015). We study a case of anonymity in practice, how it is enacted and performed in darknet 'cryptomarkets'. We use our case to challenge the current political representation of anonymity as inherently deceitful or harmful. We show how cryptomarket users create anonymity and use it as a resource that enables market interactions and allows for useful exchange of knowledge about drug consumption techniques, quality and safety. We outline our understanding of anonymity as embedded in online communities of practice, enterprises where shared knowledge and activity are emphasized over shared identity (Hobbs, 2013). Our claim is that market users assemble various technologies, some of which are designed for anonymising and some that are not, along with anonymising practices in order to operate freely on the darknet.

Anonymity can be framed in various ways: as a threat to predictable and coherent social order (Abbink & Sadrieh, 2009), an unavoidable and normal feature of daily life (Natanson, 1990), an intrinsic feature of private liberal citizenship (Froomkin, 1999), and a necessary condition of protest (Thompson, 1975). Historically, it has been assumed that anonymity is a fundamental part of the fabric of modernity with profound implications for social life. Sociology identified the emergence of anonymity as a feature of urban life (Simmel, 1903) and of a complex division of labour that necessarily involves working relationships between unknown others (Durkheim, 1893). As well as generating new forms of solidarity and self, it has also been presented as threatening social control, creating fleeting and passing interactions (Wirth, 1938) and indifference (Milgram, 1970), and leading to the creation of new forms of governance to defeat it such as surveillance assemblages (Haggerty & Ericson, 2000). Some of the assumptions behind these claims have been challenged, such as that anonymity is a general quality of urbanising societies (Gans, 1962), or that it is an inherent quality arising out of certain settings and with definite potential to promote certain kinds of usually anti-social behaviour or alienated modes of living. We join this tradition, which challenges both anonymity's supposedly a-social character and its naturalising as a technical-structural trait (Karp, 1973). We argue that in hidden communities anonymity is produced and shared as a requirement for them to function effectively.

Some features of the early debate were reproduced in relation to historical development of the internet and social media. Early libertarian and feminist conceptions saw the severing of offline and online identities as freeing humans from the weight of real world restraints and oppressions (Barlow, 1996; Spender, 1995). The cypherpunk movement sought during the 1980s and 1990s to embed a libertarian concept of cyberspace, developing cryptography and trust mechanisms that were intended to replace or resist central control and management and to substitute it with network-based systems (Branwen, 2015). The development of public encryption using Pretty Good Privacy (PGP) by Phil Zimmerman was a key moment in this. Zimmerman was subject to a criminal investigation under the US Arms Control Export Act, high strength encryption being considered a military technology. Ensuring public encryption is available and usable is part of a political movement that has related tendrils such as the campaign to retain net neutrality. There is a 'politics of code' where struggles over concepts like privacy are embedded in software and technical processes. Promoting or weakening end-to-end encryption is an argument about both security and power (Hales, 2014). That is reflected in the various positions security agencies have come to in relation to encryption as a widespread security enhancing feature without which the modern, social internet would not be possible (Moore & Rid, 2016).

Coinciding with the rise of social media, there has been a greater cultural and political focus on online anonymity as personally malign (UN Broadband Commission for Digital Development, 2015), supposedly promoting a range of damaging behaviours and stances from uncivil discourse to abuse (Reader, 2012). Political discourse in the UK, USA, China, Russia and India, among other countries, frames it as a shield and encouragement for terrorists, hackers, traffickers and trolls, people who post online in a deliberate attempt to damage individuals and online communities (Department of Electronics and Information Technology, 2015). Encryption has become the focus of some of these discussions as a problem technology. The Russian government has systematically tried to disrupt some anonymising systems whereas US government agencies been more circumspect and are constrained by unresolved legal questions (Çalışkan, Minárik, & Osula, 2015). These differences and disputes highlight the dual nature of the internet, both allowing counter-publics to emerge and also opportunities for state and private domination through control of the data infrastructure (Garrett, 2006; Maddox, Barratt, Allen, & Lenton, 2016). Researchers have identified new orientations and identities coming into being on the internet such as crypto-freedom, which to an extent promotes an older vision of the internet as composed of self-reliant, technically proficient actors and peer generated communities (Beer & Burrows, 2010; Coleman & Golub, 2008). Many users respond with resignation to the brute fact of surveillance that is embedded in the infrastructure of the internet (Lee & Cook, 2015). It is technically and personally difficult for an individual to separate their real world identity and their online personae in order to maintain anonymity, even when it is experienced as a pressing use for them.

We argue that focusing on particular technologies and on anonymity as a singular practice can be misleading. Anonymity can be broken down into different qualities that can be more suited to some activities and orientations than others (Pfitzmann & Hansen, 2010). Often it is used to mean pseudonymity, when individuals have a consistent, but disguised, persona. Multiple pseudonymous identities can be adopted to further obfuscate identity, to create desired effects through for example sock puppetry, creating multiple personae to give the impression of multiple support for one's viewpoint, or to emphasise different roles and

personas. De-linking separates different interactions by the same user and prevents them being connected by an outside agent. Undetectabilty disguises the content of hidden activity and unobservability the participants, such as the origin or recipient point of hidden communications. Ruppert et al (2013) usefully class digital social activity into actions and their traceability. Anonymity within the darknet preserves actions while it is intended to disrupt traceability. When we use the term anonymity here we use it to refer to the recognised state of being hidden, which includes these different aspects of anonymity, and then we use these more precise terms when picking out particular aspects of it. These different elements, though relevant, each describe a technical quality of anonymity. Previous research, not related to the darknet, into the nuances of anonymity on the internet has found a singular term to be left wanting because of the difference between a user *being* anonymous and them *feeling* anonymous (Kennedy, 2006, p. 870). Barratt's (2011) distinction between 'technical anonymity' and 'social anonymity' allows for a better understanding of the different effects of anonymity. Technical anonymity exists when individuals are untraceable: there is no link between their actions and a singular identifiable and accountable persona. Social anonymity is the shared sense of operating anonymously.

We take a case where the possibility of surveillance is keenly felt. The darknet is the set of relay systems and encryption protocols that disguise the origin, destination and/or the content of internet traffic. At the time of writing the most prominent of these is the The Onion Router (Tor) system. It was created by the US Naval Research Laboratory to enable secure government communications (Çalışkan et al., 2015). The darknet is often discussed as a cyberspace 'Wild West' but it is better conceived of as a way of using internet networks that allow for anonymous hosting and communication. Cryptomarkets combine the darknet with peer-to-peer payment systems such as bitcoin, litecoin, darkcoin and dogecoin, allowing for goods and services to be transacted using a public ledger or 'blockchain'. The cryptomarkets form a partially 'lean' infrastructure. They have limited techno-social features such as simple reputation systems, but within a much more sophisticated and rich anonymising infrastructure (Hine, 2015). Technical and social anonymity are pervasive features of the darknet. Users aim to be anonymous from each other and from the prying eyes of internet service providers, law enforcement agencies and other surveillance bodies. Cryptomarkets are often framed as the product of a few geeks and some devilish entrepreneurs. However, that focus on their technical and entrepreneurial achievements misses out how these markets came into being as a result of a combination of the technologies with structural conditions. These were the changes in illicit market structures and the meshing of illicit and licit economies called deviant globalisation (Gilman, Goldhammer, & Weber, 2011).

This is an area where anonymity is a pressing issue. Those who use the darknet see it as the price of admission. It is commonly presented as a technical problem. Cryptomarket users are presented as being engaged in a technical game of cat and mouse with law enforcement and each other. However, both aspects of this miss out the way in which anonymity is created and maintained as a social activity, and also the crucial interface between darknet systems and real life. Moving on somewhat from anonymity as a technical challenge, we want to highlight it as a way of engaging and maintaining social relationships on the darknet. We examined how important anonymity was to cryptomarket users; how they established and maintained anonymity; threats to anonymity; and how market relationships and reputations were maintained. The markets offer an additional social context that gives

users an opportunity to find and share information in what they regard as a safer environment.

Methods

This paper is part of an ongoing project researching how drug users and vendors make use of the darknet (Bancroft & Scott Reid, 2015). The project studies the darknet as a new context of drug use with its own attitudes and shared practices (Duff, 2007). Anonymity is a fundamental feature of how cryptomarkets are constructed technically, as markets, and as communities. It cuts across several infrastructures: the technical coding of market systems, the software tools used by vendors, buyers and administrators, the interaction norms of the market user forums, the interface between the market and the postal systems used for drug delivery, and the security practices of users. We aimed to understand how users maintained anonymity while navigating the markets and interacting with other users and vendors.

We had a two-stage data collection process. First, the discussion forum for what was a major cryptomarket, which we have christened 'Merkat', was accessed. The market has at the time of writing been suspended and is no longer in operation (April 2016). Permission to research was requested from the administrator but no reply was received after one month. As the forum rules did not bar researchers, and the forum was public, we decided to continue with the data collection. We lurked in the forum from March-May 2015 and manually copied forum threads into a database using the qualitative data indexing programme Nvivo. The database consisted of 152 threads, ranging from 20 to 7,000 posts each. Forum data covered the two-year period from the market's creation. We also recruited five interviewees using the personal connections of both authors and snowball sampling. Interviews were conducted both in person and by using video and secure encrypted chat methods. We sought to meet interviewees' concerns about their anonymity. This often took the form of using technical anonymity to underscore social anonymity. Although the number of interviewees was small, the interviews allowed us to collect rich data about how they approached and used the darknet.

Analysis was conducted iteratively, using a developing coding framework structured around emerging themes. In total 5,723 text elements were coded using automated and hand-coding. Codes covered market structures and processes, buyer and vendor comportment on forums, anonymising practices, trust, interfaces between systems, surveillance and law enforcement activities. Using both data collection methods allowed us to explore a much greater range of ways of using the darknet. In particular, forum users tend to be more active and serious about security. Interviewees were more of a range, from those who were more heavily involved in using the darknet and thought a great deal about anonymity to the more casual and infrequent users who relied more on the darknet working for them to protect their identity. In line with the norms of the cryptomarkets we have paraphrased forum data to ensure user accounts cannot be identified through searching. We sought to reflect users' norms and expectations in our own practice in both research and writing up (Association of Internet Researchers, 2012). User names and interview names are pseudonyms.

The satisfactions of the hidden

Cryptomarket users build a secure space in which they can experience a more satisfactory and controlled means of interacting in the drug market. There are benefits of use in terms of security, quality and the reduction in need for violence (Van Hout & Bingham, 2013a, 2014).

A consistent admonishment on the forum was not to mistake social anonymity for technical anonymity. The latter needed continual curation. The technology is used as a means to avoid violence and personal risk but it is also used to engage with others in a more palatable way. Cryptomarket sales and interactions do not have face-to-face contact but may, because of technical and social anonymity, allow for types of exchanges users are not able to have or find more difficult in offline markets. This social space allows for an atypical set of relationship constructions. The social context of market performance and subcultural capital required to buy drugs on cryptomarkets is different from offline modes of purchasing or acquiring drugs. Emphasis is placed on digital competence, speed, stealth and responsiveness, in a context where anonymity does not mean there is no accountability.

Many forum discussions concerned security and its potential breaches. Users and vendors compared notes and discussed stealth. Vendors were rated on their stealthiness and this was the basis for many discussions. We asked interviewees to describe the whole process from initial exploration through purchasing and delivery. Interviewees gave detailed accounts of how they went about using the darknet and their motivations for using it. Forum discussions were only one place where information about anonymity was exchanged. Related clearnet sites such as reddit hosted extensive discussions of security and users frequently posted warnings and advice there. As well as these practical orientations, users gain personal satisfaction from successfully using the darknet while maintaining anonymity and vendors show their customer service quality by engaging in security signalling.

The role of forum administrators in managing relationships between participants was contested. They would block and ban individuals from engaging in forum communications for various real and alleged transgressions (Holt, Smirnova, Chua, & Copes, 2015). Some users alleged that many of these actions were motivated by personal interest rather than a desire to protect the integrity of the market. Forums facilitated 'nested support systems' that provide a place for information exchange, connections with other users and mutual support from those that have or have experienced similar difficulties (Van Hout & Bingham, 2013b). Less experienced users are able to benefit from forum sections that have 'how to' instructions, and it is possible to find out which vendors have better products or more secure packaging (Martin, 2014).

Interviewees recalled discovering and becoming involved with the darknet as a moment when their technical skills could be used. The recognition of the darknet as a potentially risky place was acknowledged as a challenge that could be overcome by using the right combination of trust practices and checks. Scamming was expected, but in practice it was more common for consignments to go astray than for users to fall victim to scam vendors or sites.

> *Well I was always interested in things like bitcoin and then I found out about Tor and things like that expanded like the knowledge base of it and then I found out just how open it was. I went onto the hidden wiki which is a site which used to document loads of Onion [Tor] sites. That's dead now, that's been hacked, so it's just loads of scam sites now which I found out to my cost. They had this huge list of things like, you could get people assassinated on the internet … I mean it's not something I'm interested in but wow [laugh], it's the knowledge that you can. So yeah, I gravitated*

> *towards like, hey I could get my weed really cheap delivered to me from the Europe. And yeah ended up getting into it from there. Interviewee 'Al'*

Interviewees and forum users described the personal satisfaction that came from avoiding surveillance and showing one's digital nous. Interacting with others online can allow for membership of a subculture without the risk of stigma or exposure that might be associated with the related activity in a more visible setting (Adler and Adler 2008). Users who were sufficiently savvy and confident could take on a technology management role where their skills were acknowledged by others. They mediate and broker the street-cryptomarket relationship. One interviewee did this by selling his digital skills to local dealers, another by using them for social supply.

We suggest that the type of activity made possible by darknet hidden services is best conceived of as not being limited to specific instances of law breaking or interactions with others online. Rather, darknet markets and forums provide technically proficient users with another space in which to exist socially, a different outlet for interactions that are made difficult or impossible by their circumstances when not online. It provides space for a community of technically skilled individuals to thrive.

Technical anonymity hinges on an empirical question: is it possible for someone to connect a darknet user's activity to their legal identity? If the answer is 'no' then they have technical anonymity, if they can be then they do not have technical anonymity – a binary outcome. With social anonymity, the user's own perception of being anonymous is determined by a combination of factors. The extent of the user's technical knowledge and skill will determine how well they combine various anonymising techniques and software applications to avoid detection. One interviewee had used cryptomarkets with someone else guiding the main technical elements, and reflected on how the techniques involved had to be continually re-learnt and shared with others in order to be sure of their effectiveness:

> *The fact that you're giving people your address over the internet to buy class A drugs is also something I wouldn't want to do without fully understanding how it works. And then also hiding your IP [internet protocol] address, because you know that government, governments and stuff like that are monitoring these sites like you know that they are monitoring the traffic, let's not lie about that. And so you want to be able to hide your IP and stuff like that effectively and know you've hidden it well and I would just be relying on what I'd read on the internet basically to understand that I'd hidden myself well enough and I don't feel that's good enough. Interviewee 'Sel'*

More experienced users are more likely to feel secure in their methods to ensure security and to enjoy the benefits of being able to engage with likeminded people. When users experience social anonymity, they are able to engage in the forums without the inhibitions experienced when fearing the exposure of information that will lead to social stigma or self-incrimination.

Attesting persona

Users have personas without being identifiable. Vendors benefit from establishing consistent but disguised personae. The expectation that users who wish to buy and sell on

the darknet maintain a consistency of behaviour and etiquette towards other users shows the difference from what might be expected from a large face-to-face criminal marketplace. Though a vendor will strive to completely separate their profile from their legal identity and 'public' life, the markets are structured so that trust is built up through user reviews. Buyers expect sellers to live up to the records of their previous transactions recorded prominently on each vendor's profile and in the associated discussion forums. Darknet market users try and ascertain the consistency and continuity of the vendor's identity. In this instance, the continuity of a persona and its 'attestability' by others is key to acceptability and trustworthiness. Well-known vendors would establish themselves across different markets and market administrators would allow for this by reserving the usernames of well-known vendors when a new site was created. Administrators would pre-register them and allow them to transfer their feedback to the new site. Good vendors would have an entourage of users on the site attesting to their reliability. Buyers use sites like reddit and Grams that aggregate and index across different markets.

Multiple identities are a challenge for users and vendors:

> *Lol, it must be a mess having to keep up these shills [false accounts], you chubby little loser. Perhaps I could call you out with your Christian name? Or get the cops? Have you worked out how I am yet, wanker? No chance – you don't recognize your own mug in the mirror. Forum user 'vphelps'.*

Holding multiple personas across different markets could be interpreted benignly. Having several in the same market was thought to be suspicious and the act of scammers, fake vendors and hostile vendors producing smack talk about rival vendors. So although anonymity was prized, singularity was as well – in the sense of vendors having a single, pseudonymous identity with which they could be held to account. Users valued having one voice and one chain of responsibility.

The salience of anonymity varied among users. Some users had an active, 'total' approach to anonymity and would for example use anonymising methods when viewing clearnet sites that hosted information about the darknet. Others took a more relaxed approach and assumed that much of the work was done for them by the market itself and the software they used to access it. Anonymising was both practical and a moral norm, as shown by the response to its opposite. Doxxing is when a person's anonymous online persona is linked with their real world identity and address. Some vendors make threats of doxxing but this is mostly seen as beyond the moral norms of the community and akin to snitching. Partial doxxing could be a threat:

> *I know that was an over-reaction but I had run out of options. This user has been trying to wreck my reputation. Merkat forum mods wouldn't do anything. So I let the person know that I had his full address and he should drop it. I never gave out their complete doxx despite what the Merkat mods say. I just gave out part of their phone number – nothing that would doxx them. Vendor 'Pigtime'.*

On the one hand doxxing is forbidden. On the other, forum users will claim a knowledge of a vendor's real world identity to call out scammers. One approach was to identify the vendor consistently through these different personae without doxxing them. Doxxing was technically possible for vendors and market administrators, however it was a rare occurrence. The threat of doxxing to community social anonymity was greater than any passing benefit from doxxing an individual.

Maintaining opsec through defeat and deniability

The total process for securing transactions on the darknet was 'opsec' (operational security). As forum users often reminded each other, opsec was active, not passive. Using the right software on its own would not guarantee functioning opsec. Vendors had to apply opsec principles to the parts of the supply chain that were in their control. It could easily be compromised. Sloppy practices included using the same username in darknet and clearnet sites, and using clearnet email addresses for darknet transactions. Buyers of smaller amounts felt freer to opt-in to some opsec practices.

We have sorted the techniques used by cryptomarket users into two: technical defeat and socio-legal deniability. Defeat techniques are the kind of encryption, stealthing and evasion that shields them from the gaze of law enforcement. 'Tumbling' bitcoin to ensure it was not traceable is a technique of defeat. Without tumbling, users can be traced through the blockchain if another part of the transaction is compromised. It is a form of money laundering, and could be done through a service like Bitcoin Fog that effectively creates a break in the chain through which users can transfer funds to different wallets to pay vendors, or payment can be transferred directly to the vendor's wallet. Some users saw it as overkill for the casual buyer.

There was a sense among more involved users that defeat on its own was inadequate. As Al pointed out, there were too many potential security holes:

> *Everyone would view reddit through Tor or something so unless they are an idiot of course … There are other mechanisms for them to track you, using cookies or javascript that could be used to track you. But if you're on something like Tails [an anonymous computer operating system], that's automatically blocked anyway. So if someone was to view it on it, even through Tor, they would still be trackable, even if you maximise the screen then the website can tell the resolution of your monitor ... So you can't have anything maximised, ever. So they would know exactly the size of the screen, right 'someone viewed this with a resolution of this, you had a resolution of X, so we have reason to believe that was you'. And obviously that's not going to work on its own, you need other evidence but that is circumstantial. There's actually a specific warning when you go to maximize a window on Tails, it says 'hey maybe not'. Interviewee 'Al'*

Ideally PGP encryption is used when sending buyers' addresses to vendors – so it should not be linked to the purchase directly through the market. When vendors are arrested, suspicion is expressed on reddit that they may have kept buyers' details. In contrast, some users were very relaxed about opsec, using their own computers with a mainstream operating system, Tor, and having drugs delivered to their home address. The different approaches our interviewees took demonstrated the performative aspect of anonymising, where being fully in control of one's own digital trail was a pleasure in itself.

Deniability is a way of engineering interactions that involves severing personal legal responsibility for drug shipments and introducing plausible deniability. For example, using a false name for deliveries and scrubbing stored addresses is a technique of deniability, as is wording messages in a deliberately vague way.

> *[Discussion of secure email systems] I've been told that particular server has been infiltrated by the NSA [US National Security Agency] as well. To be safe always avoid the kind of words that might trigger a search. I make sure I'm VERY vague in emails. Forum user 'Hilarysgusset'*

Much of the discussion around security on the darknet focuses on techniques of defeat. However, arrests are more likely to happen because of failures of deniability: being caught with large quantities of drugs clearly destined for consignment, making large cash purchases, having others give evidence leading to a warrant and so on.

Defeat on the vendor's side involves stealth. Good stealth is an important measure of vendor quality. Shipping in good 'cover', such as a DVD case or another innocuous item, is praised, as is having a legitimate-looking return address. The more the package appears to be a plausible shipment from an online retailer the better. Vacuum sealing, use of moisture barrier bags, and good practice such as cleaning vacuum seals, are commented on. Good stealth is held to go right through the supply chain and involves the vendor using untraceable systems when paying for postage. The technique of defeat is also key here, ensuring no link in the chain of identification will lead back to the vendor.

The inadequate shield of technology

Two technology backbones underpin the cryptomarkets. The internet backbone – the system of routers and cabling connecting the different hosts around the world – and the global postal system. Each could link the users to their real world identities in various ways and vendor and user opsec was crucial in stopping this from happening. Successful use of the technology was a combination of the right hardware, software and good practice. There were a set of technologies and infrastructures involved, from specialised software, burner phones and the postal service. Encryption which scrambles the data packets being sent via the internet backbone is the magic invisibility cloak that 'noobs' (new, inexperienced users) are constantly being reminded about on the forum.

> *The first time as a vendor was on Evolution. I set up a simple vendor page, not much on there because I didn't think much needed to be said. After the first few orders were sent in unencypted I told the buyers never to do that. I put a post in all my listings – use PGP or don't order. It was amazing how many people don't bother with the simplest encryption. Vendor 'diamondsogs'*

However anonymity is not synonymous with encryption. Embedded metadata in a document can reveal much about its author. Data embedded in photos records the camera type, date, time and often the location unless this metadata is stripped out or not recorded in the first place (Julian, 2015). Frequently using the right technology could lead to lax real world security practice. Real world security holes were neglected as long as the person thought they had got the digital security set up correctly.

Bitcoin is often represented as a technology of anonymity. Unlike Tor it is not designed for anonymity, but it does permit it (Reid & Harrigan, 2013). Various techniques and practices have to be applied to make bitcoin anonymous. The first possible identity leak is at the point of converting government backed fiat currency such as British sterling or the US dollar into cryptocurrency. Law enforcement can follow the blockchain and monitor large transactions that can then be matched up with darknet users using brute force data matching. One method of de-linking is to use local bitcoin:

> *[Bitcoin vendor] picked me up, drove to another cafe, bought a pot of tea while we had a little chat about Bitcoin and the general crypto-economy and all that jazz because the transfer was taking a while to come through. The transfer came through, and there was a verification code that I knew but he wouldn't get until he had sent the coins and the transaction had been confirmed. So he then showed me the code and they matched up with one that I already had, so I knew the Bitcoins had been transferred successfully. And I was able to go home. Interview 'Al'*

There is a theatre of security aspect to some of the precautions taken by interviewees, vendors and forum users, where anonymising activities become ritualised (Amoore & Hall, 2010). Security practices are part of the expected comportment when interacting with the market. There is similarity with the legal security market (Loader, Goold, & Thumala, 2015). Many of the techniques used are part of security signalling. Security measures by vendors are a signal of the vendor's reliability and professionalism. Those who did not work opsec throughout the supply chain were seen as amateurish. Security signalling is part of the theatre of security that has become a common part of social life in many societies. Public and private security services engage in a variety of techniques that signal that they are taking security seriously. As security has become privatised and spread throughout society, these theatres of security are becoming more common (Schreier & Caparini, 2005). Darknet vendors adopted security signalling as mark of vendor and product quality. In addition to signalling, personal pride and social status can come from successfully handling the layered systems of encryption and anonymisation. Rituals of anonymising could also be seen as disrupting the normalised, ritualised surveillance which has been embedded in the fabric of social life (Bajc, 2007). In these ways, anonymity becomes a resource for both sellers and buyers, who use it to signal quality, trustworthiness and competence.

Discussion

Various implementations of encryption are presented as troublesome technologies that encourage a dangerous anonymity that is corrosive of the social order. As we have shown, this misrepresents both the history of those technologies and how they are used today. Treating anonymity as inherently suspicious brushes aside critical perspectives that point to government mandated publicity of individual identities and behaviours as a tool of social control (Cobb, 2007), which are features of new forms of governance that target conduct (Flint & Nixon, 2006), and to the ethics of cryptography (Rogaway, 2015). There is also a long history of anonymising practices and technologies being tools with a political purpose (O'Brien, 2001; Williams, 1986). We started with the argument that anonymity, often presented as a kind of withdrawal from social life is through and through a form of social engagement (Marx, 1999). It severs the relationship between one persona and others and allows them to vary and adapt to different arenas (Shilling & Mellor, 2015). It is not easy to attain and maintain anonymity online. Supposedly anonymised individuals can be de-anonymised using metadata with relative ease (Ohm, 2010) or through the normal workings of internet service providers. Currently there are concerted attempts by some states and corporations to collapse multiple online personas into one traceable identity. However, users' deniability practices can disrupt de-anonymising techniques (Spitter, Klaver, Koot, & van Staalduinen, 2015).

As well as challenging the representation of anonymity as deceitful, we also challenge the representation of its opposite as trustworthy. Various governments have sought to establish the measure of trust as the permanence and openness to surveillance of an individual's identity. Governments and private actors seek to link individuals' online personae with their offline identity. These developments are part of the generalisation and privatisation of surveillance and securitisation of everyday life. More and more private organisations are expected to be involved in immigration control, tracking and monitoring extremism and so on. Though this has been represented as privatisation, it might be better to call it nationalisation of the internet and associated technologies by various states from China to Russia. There is a tension in the online world between requirements that users are consistently traceable to a singular, real world self, and encouraging users to adopt multiple identities. We can then question the classical sociological assumption that there is a one to one mapping between 'self' and 'identity' when dealing with multiple, fluid selves.

In contrast to users of the clearnet (Viseu, Clement, & Aspinall, 2004), our respondents are concerned to hide their activities and identities. This presents a new set of problems in establishing trust. Instead of achieving trust through connecting to a real world identity, the measure of trust is the attestibility and continuity of the online persona. For many darknet users, the ability to remain anonymous is a form of resistance. Mostly, the anonymity of the darknet was not deceitful. Anonymity does not preclude developing social relationships and mutual support between buyers and vendors. In this article we have highlighted the growing politics of anonymity, through one setting where anonymity is an expected feature of interaction. Anonymity produces some challenges for users in maintaining trust, however it is not fundamentally debilitating. Anonymity at first sight potentially challenges some assumptions about social life, particularly the one-to-one mapping of personal, legal and moral accountability. However darknet users were keen to maintain a consistent identity. This was necessary for vendor and customer reputation and ensuring trust (Vickery, 2015).

Public discussion of anonymity is dominated by privacy related concerns over surveillance, and the uses of anonymity as a shield for harmful behaviour. Both of these perspectives see anonymity as an individual quality, that disrupts the connection between online and offline personas. We have discussed a setting where anonymity is used to create lateral connections between individuals. It allows for community to be performed and stigma to be challenged. We do not wish to downplay the problems caused to individuals and online communities by unaccountable negative behaviour and malicious internet traffic originating in the darknet. However, we challenge the assumption that technical anonymity is the prime facilitator of this behaviour, and that the way to stop it is to de-anonymise the darknet. Doing so would damage the interests of minority communities and contribute to the general decline of privacy in contemporary life on- and off-line.

While not exactly comparable, evidence from peer-to-peer file-sharing suggests that well-publicised threats of deanonymisation and prosecutions have only a limited deterrent effect on illicit behaviour of this kind, instead leading users to develop more sophisticated techniques and technologies to remain hidden (Lysonski & Durvasula, 2008). In a similar way, what was central in our study was how the cryptomarket vendors and buyers combined technology, opsec and interaction norms to maintain a hidden community. It is also the case that despite its significance in public discussion of the darknet anonymity is not a necessary condition for online drug trading (Watters & Phair, 2012) and many forms of drug trading go on using the internet, and especially social media, without those involved

going to great lengths to disguise their real world identities from each other or possible third parties. Indeed, the darknet receives a significant amount of attention from law enforcement agencies and is far from being impenetrable. Being part of a hidden community on the darknet provided benefits that went beyond being able to buy and sell drugs in relative security. Vendors and buyers preferred its greater predictability and accountability, and the fact that it allowed them to demonstrate and be acknowledged for interpersonal, professional and technical skills in way that was difficult or impossible in face to face or open internet drug exchanges.

Acknowledgements

Thanks to Steve Kemp, Kimberley Masson, the anonymous reviewers, and our research participants.

Bibliography

Abbink, K., & Sadrieh, A. (2009). The pleasure of being nasty. *Economics Letters*, *105*(3), 306–308. http://doi.org/10.1016/j.econlet.2009.08.024

Amoore, L., & Hall, A. (2010). Border theatre: on the arts of security and resistance. *Cultural Geographies*, *17*(3), 299–319. http://doi.org/10.1177/1474474010368604

Association of Internet Researchers. (2012). *Ethical Decision-Making and Internet Research - Recommendations from the AoIR Ethics Working Committee (Version 2.0)*. Retrieved from http://aoir.org/reports/ethics2.pdf

Bajc, V. (2007). Surveillance in public rituals: Security meta-ritual and the 2005 U.S. Presidential Inauguration. *American Behavioral Scientist*, *50*(12), 1648–1673. http://doi.org/10.1177/0002764207302473

Bancroft, A., & Scott Reid, P. (2015). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy*, *early online*. http://doi.org/10.1016/j.drugpo.2015.11.008

Barlow, J. P. (1996). A declaration of the independence of cyberspace. Retrieved from http://homes.eff.org/~barlow/Declaration-Final.html

Barratt, M. J. (2011). Discussing illicit drugs in public internet forums: Visibility, stigma, and pseudonymity. In *Proceedings of the 5th International Conference on Communities and Technologies* (pp. 159–168). Brisbane. http://doi.org/10.1145/2103354.2103376

Beer, D., & Burrows, R. (2010). Consumption, Prosumption and Participatory Web Cultures: An introduction. *Journal of Consumer Culture*, *10*(1), 3–12. http://doi.org/10.1177/1469540509354009

Beer, D., & Burrows, R. (2013). Popular Culture, Digital Archives and the New Social Life of Data. *Theory, Culture & Society*, *30*(4), 47–71. http://doi.org/10.1177/0263276413476542

Branwen, G. (2015). Silk Road: Theory & Practice. Retrieved from http://www.gwern.net/Silk%20Road

Çalışkan, E., Minárik, T., & Osula, A.-M. (2015). *Technical and Legal Overview of the Tor Anonymity Network*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Cobb, N. (2007). Governance through Publicity: Anti-social Behaviour Orders, Young People, and the Problematization of the Right to Anonymity. *Journal of Law and Society*, *34*(3), 342–373.

Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255–277. http://doi.org/10.1177/1463499608093814

Department of Electronics and Information Technology. (2015). *Draft National Encryption Policy*. New Delhi: The Indian Ministry of Communications and Information Technology.

Duff, C. (2007). Towards a Theory of Drug Use Contexts: Space, Embodiment and Practice. *Addiction Research & Theory*, *15*(5), 503–519.

Durkheim, E. (1893). *De la division du travail social*. Paris: Les Presses universitaires de France.

Flint, J., & Nixon, J. (2006). Governing Neighbours: Anti-social Behaviour Orders and New Forms of Regulating Conduct in the UK. *Urban Studies*, *43*(5–6), 939–955. http://doi.org/10.1080/00420980600676386

Froomkin, A. M. (1999). Legal issues in anonymity and pseudonymity. *The Information Society*, *15*(2), 113–127.

Froomkin, A. M. (2015). From Anonymity to Identification. *Journal of Self-Regulation and Regulation*, *1*, 121–138.

Gans, H. (1962). *Urban Villagers: Group and Class in the Life of Italian-Americans*. New York: The Free Press.

Garrett, R. K. (2006). Protest in an Information Society: a review of literature on social movements and new ICTs. *Information, Communication & Society*, *9*(2), 202–224. http://doi.org/10.1080/13691180600630773

Gilman, N., Goldhammer, J., & Weber, S. (2011). *Deviant globalization: Black market economy in the 21st century*. London: Bloomsbury Publishing.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605–622. http://doi.org/10.1080/00071310020015280

Hales, T. C. (2014). The NSA Back Door to NIST. *Notices of the AMS*, *61*(2), 190–192.

Hine, C. (2015). *Ethnography for the Internet: embedded, embodied and everyday*. London: Bloomsbury Academic.

Hobbs, D. (2013). *Lush Life: Constructing Organized Crime in the UK*. Oxford: Oxford University Press.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103. http://doi.org/10.1080/17440572.2015.1013211

Julian. (2015). Deanonymizing Darknet Data. Retrieved from http://atechdad.com/deanonymizing-darknet-data/

Karp, D. A. (1973). Hiding in Pornographic Bookstores: A Reconsideration of the Nature of Urban Anonymity. *Urban Life and Culture*, *1*(4), 427–451.

Kennedy, H. (2006). Beyond anonymity, or future directions for internet identity research. *New Media & Society*, *8*(6), 859–876. http://doi.org/10.1177/1461444806069641

Lee, A., & Cook, P. S. (2015). The conditions of exposure and immediacy: Internet surveillance and Generation Y. *Journal of Sociology*, *51*(3), 674–688. http://doi.org/10.1177/1440783314522870

Loader, I., Goold, B., & Thumala, A. (2015). Grudge spending: the interplay between markets and culture in the purchase of security. *The Sociological Review*, *63*(4), 858–875. http://doi.org/10.1111/1467-954X.12329

Lysonski, S., & Durvasula, S. (2008). Digital piracy of MP3s: consumer and ethical predispositions. *Journal of Consumer Marketing*, *25*(3), 167–178. http://doi.org/10.1108/07363760810870662

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society*, *19*(1), 111–126. http://doi.org/10.1080/1369118X.2015.1093531

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice*, *14*(3), 351–367. http://doi.org/10.1177/1748895813505234

Marx, G. T. (1999). What's in a Name? Some Reflections on the Sociology of Anonymity. *The Information Society*, *15*(2), 99–112.

Milgram, S. (1970). The Experience of Living in Cities. *Science*, *167*(3924), 1461–1468.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, *58*(1), 7–38. http://doi.org/10.1080/00396338.2016.1142085

Natanson, M. (1990). Anonymity: A study in the philosophy of Alfred Schutz. *Human Studies*, *13*(1), 97–101.

O'Brien, J. (2001). Putting a Face to a (Screen) Name: The First Amendment Implications of Compelling ISPs to Reveal the Identities of Anonymous Internet Speakers in Online Defamation Cases. *Fordham Law Review*, *70*, 2745.

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, *57*, 1701–1777.

Pfitzmann, A., & Hansen, M. (2010). *Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology*.

Dresden: TU Dresden, Faculty of Computer Science, Institute of Systems Architecture.

Reader, B. (2012). Free Press vs. Free Speech? The Rhetoric of 'Civility' in Regard to Anonymous Online Comments. *Journalism & Mass Communication Quarterly*, *89*(3), 495–513. http://doi.org/10.1177/1077699012447923

Reid, F., & Harrigan, M. (2013). Security and Privacy in Social Networks. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, & A. Pentland (Eds.), *An analysis of anonymity in the bitcoin system* (pp. 197–223). New York: Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4614-4139-7_10

Rogaway, P. (2015). The Moral Character of Cryptographic Work. Retrieved from http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

Ruppert, E., Law, J., & Savage, M. (2013). Reassembling Social Science Methods: The Challenge of Digital Devices. *Theory, Culture & Society*, *30*(4), 22–46. http://doi.org/10.1177/0263276413484941

Schreier, F., & Caparini, M. (2005). *Privatising security: Law, practice and governance of private military and security companies*. Geneva: Centre for the Democratic Control Armed Forces. Retrieved from http://www.dcaf.ch/content/download/34919/525055/version/1/file/op06_privatising-security.pdf

Scott, C. R. (2004). Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations. *Free Speech Yearbook*, *41*(1), 127–141. http://doi.org/10.1080/08997225.2004.10556309

Shilling, C., & Mellor, P. A. (2015). For a Sociology of Deceit: Doubled Identities, Interested Actions and Situational Logics of Opportunity. *Sociology*, *49*(4), 607–623. http://doi.org/10.1177/0038038514546661

Simmel. (1903). The Metropolis and Mental Life. In J. Farganis (Ed.), *Readings In Social Theory: The Classic Tradition To Post-Modernism* (pp. 149–157). New York: McGraw Hill.

Skeggs, B., & Yuill, S. (2015). The methodology of a multi-model project examining how Facebook infrastructures social relations. *Information, Communication & Society*, *Early online*. http://doi.org/10.1080/1369118X.2015.1091026

Spender, D. (1995). *Nattering on the net: Women, power and cyberspace*. Melbourne, Vic: Spinifex Press. Retrieved from http://dl.acm.org/citation.cfm?id=525249

Spitter, M., Klaver, F., Koot, G., & van Staalduinen, M. (2015). Authorship Analysis on Dark Marketplace Forums. In *Proceedings of the IEEE European Intelligence & Security Informatics Conference (EISIC)*. Manchester.

Thompson, E. P. (1975). The crime of anonymity. In D. Hay, P. Linebaugh, J. G. Rule, E. Thompson, & C. Winslow (Eds.), *Albion's Fatal Tree: Crime and Society in Eighteenth-Century England* (pp. 255–344). London: Allen Lane.

UN Broadband Commission for Digital Development. (2015). *Cyber Violence against Women and Girls: A World-Wide Wake-Up Call*. Geneva: Broadband Commission for Sustainable Development.

Van Hout, M. C., & Bingham, T. (2013a). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy*, *24*(5), 385–391. http://doi.org/10.1016/j.drugpo.2013.01.005

Van Hout, M. C., & Bingham, T. (2013b). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy*, *24*(6), 524–529. http://doi.org/10.1016/j.drugpo.2013.08.011

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, *25*(2), 183–189. http://doi.org/10.1016/j.drugpo.2013.10.009

Vickery, J. R. (2015). 'I don't have anything to hide, but … ': the challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, *18*(3), 281–294. http://doi.org/10.1080/1369118X.2014.989251

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating Privacy Online. *Information, Communication & Society*, *7*(1), 92–114. http://doi.org/10.1080/1369118042000208924

Watters, P. A., & Phair, N. (2012). Detecting Illicit Drugs on Social Media Using Automated Social Media Intelligence Analysis (ASMIA). In Y. Xiang, J. Lopez, C.-C. J. Kuo, & W. Zhou (Eds.), *Cyberspace Safety and Security* (pp. 66–76). Berlin: Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-35362-8_7

Williams, D. (1986). *The Rebecca Riots : a study in agrarian discontent*. Cardiff: University of Wales Press.

Wirth, L. (1938). Urbanism as a Way of Life. *American Journal of Sociology*, *44*(1), 1–24.