4

DEATH BY SWAT: THE THREE ELEMENTS OF SWATTING

John Bahadur Lamb

The internet has become so ubiquitous in our lives that much of our commerce, socialising, dating and recreation are now carried out via electronic means (Katz & Rice, 2002). Such a growth in both traffic and time spent on the internet has seen new platforms emerge that allow individuals to easily cross the boundary from analogue reality to digital fantasy. This could be through the careful management of a social media page to present a fictitious account of one's life via platforms such as Facebook, *Twitter* and Instagram, or it could be the broadcasting of personal performance in order to experience celebrity via platforms such as *YouTube*, *Vimeo* and *Twitch.tv*. Whilst

these digital portrayals are often carefully managed and do not reflect reality, there is a burgeoning market of consumers who are willing to monetise the performances which people share, and it is estimated that social media influencers generate $1.7 billion for the global economy each year (Media Kix, 2017).

However, whilst money is a driving force of much of what occurs over the aforementioned digital platforms, there is a darker side to this growing digital market place. As has been well-documented, there are numerous illicit markets available on the internet which sell everything from fake handbags (Radon, 2012), weapons (Copeland, Wallin, & Holt, 2019), narcotics (Van Hout & Bingham, 2013) and even child abuse imagery (Davidson & Gottschalk, 2010). Yet we must not think of the internet as easily dividable into licit and illicit as there are numerous areas of human interaction played out via digital means which operate in the grey areas between the two. One such example of such liminal activities is the humble prank.

Usually harmless, pranks are often thought of as being a mildly mischievous act which embarrasses or inconveniences the victim (Merriam-Webster, 2020) for the amusement of an audience who are physically present at the scene of the prank. With the advent of the internet and the ability to publish or even live stream video, pranks are able to to reach a much larger audience as physical presence is no longer needed. When this amplification of audience numbers comes the ability to monetise these online performances via advertising revenue earned as individual's accessing the web pages which are hosting the videos or live stream (Taylor, 2018). One good example of this process is that of Jackass who were a crew of pranksters who started their careers creating home-shot videos of pranks, were then talent-spotted and were given a TV show by MTV and many of whom have gone on to have successful multi-million dollar Hollywood careers (Spitz, 2010). However, the ability to make significant money from online

performances also means that this new market place is open to exploitation by those who are motivated by jealousy, revenge or who see an opportunity for criminal activity (Jaffe, 2016).

An example of one such marketplace is *Twitch.tv* which is a streaming website that allows users to create a page via which they can share live videos of them performing. These performances usually take the form of allowing audience members to watch the *Twitch.tv* page owner playing a computer game at a very high level whilst providing an audio commentary. This is then monetised via audience members being able to tip the performer, pay for a subscription to the performers feed and even buy merchandise from them (Twitch.tv, 2019). Significant amounts of money can be made by successful *Twitch.tv* performers, with the top level earners often becoming partners to the website and gaining corporate sponsorships worth thousands of dollars (Taylor, 2018).

Twitch.tv is a live stream which often shows a video feed of both the gameplay action and the performer with many fans choosing to watch certain performers because of the quality of the reactions that the performers have. This immersive visualisation creates an intimate consumptive space which allows those who are watching the stream to experience the gameplay as if they were physically present with the performer rather than separated by large distances. In turn, fans will often give performers larger tips or purchase more merchandise, should the performer engage with them personally either via audio chat or via text as they are performing. As such, the interactions between fans and performers can often be highly personalised with virtual communities forming around certain games, certain performers or even certain genres of game (Taylor, 2018). As with any community, these *Twtich.tv* groups often become quite tight knit with their own language, expected behaviours and shared jokes. It is this shared socialisation that creates the space in which virtual and

analogue realties begin to overlap and new forms of deviance can be seen to emerge with one such form of deviance being the act of 'swatting'.

Swatting is a form of deviant behaviour, currently only present in the United States, which blurs the line between the prank, criminal activity designed to harm an individual and social policing effort. This is partially due to the motivations of the individual who triggers a swatting and partially because the outcome of swatting cannot be predicted in the same way that the outcome of most traditional pranks can. The act of swatting consists of an individual calling the police, identifying as somebody else who is perpetrating a situation that is almost certainly going to lead to the loss of innocent lives, such as an armed hostage situation. The individual then gives the address of the person they have identified themselves as and watches via a live stream online as the police respond (Calabro, 2018). Now, it is important to note that when swatting is used as a prank, it is a performative act which is specifically designed to be visually consumed by others who are already watching the victim via platforms such as *Twitch.tv*. This separates swatting from more traditional prank calls to the police, which did not have the visual element and which only provided deviant amusement to the individual who was actually making the phone call. Thus, swatting can be thought of as both a prank and a violent usurpation of the performative workspace of the victim which refocusses the audience's attention away from the victim and onto the perpetrator who will often take ownership of the event via their online alias (Calabro, 2018). The reasons for using swatting to carry out such a refocussing of the performative work space through police-mediated violence can be numerous with the perpetrator seeking humour, revenge, to discredit the victim (FBI, 2008) or potentially to create a fake incident which serves a politically violent purpose (Enzweiler, 2015).

However, in order for the refocussing to be successful, the act of swatting needs to be a dramatic, almost cinematic event which captivates the online audience. In order to achieve this, the perpetrator purposefully chooses a crime which will see the police deploy a SWAT team. Standing for Special Weapons and Tactics, SWAT teams (and other Police Paramilitary Units (PPUs) under other names across the United States) were originally created in 1960s Los Angeles to respond to crimes which ordinary patrol officers are not equipped to deal with (Kraska & Kappeler, 1997). Since then these teams have spread across law enforcement in the United States and are highly trained, paramilitary style specialist officers who are tasked to the most dangerous situations. Such situations often require SWAT teams to undertake explosive entry into premises which involves the use of breaching charges or shotguns to force doors and stun grenades to temporarily disorientate the perpetrator so as to allow the officers to affect a safe arrest (Kraska & Kappeler, 1997). Should the SWAT team believe that life is in immediate danger, then the SWAT team members will not hesitate to use lethal force to ensure that individuals are protected from harm (Kraska & Kappeler, 1997). The perpetrators of swatting are aware of these capabilities and the cinematic effect that they can have and, thus, they only call in crimes which are likely to see a SWAT team respond.

There is an inherent danger to a SWAT team responding to what they believe to be a crime where loss of life is imminent. Whilst SWAT teams exist to protect life and have an inherent flexibility that allows them to respond as events play out on the ground, they are a paramilitary style force which has standard operating procedures (SOPs) which dictate their initial response (Kraska & Kappeler, 1997). Along with these SOPs is a rigorous training regime which sees the SWAT teams rehearse how they will carry out such things as hostage rescue or dealing with an active shooter (Kraska & Kappeler, 1997).

As Waddington (1993) has argued, these two things combine to create a military like culture where speed, aggression and surprise are favoured over the more traditional policing approach of talking in order to deescalate the situation. In turn, this creates an approach which sees the potential perpetrator as a bad guy or enemy who must be defeated in order to protect the potential victims (Waddington, 1987). If we then apply this to a swatting situation, it becomes unsurprising that in at least two instances the act of swatting has led to the death of the individual who has been victimised.

For example, in Wichita in 2017, local patrol officers ended up responding to a swatting incident that led to the loss of life for the victim, Mr Andrew Finch. An innocent individual, Andrew Finch, ended caught up in a minor disagreement over a $1.50 bet that had been made on the outcome of an online match in the video game *Call of Duty: WWII* (Sledgehammer Games, 2017; Statt, 2017). As a result of this disagreement, Tyler Barriss placed a call to local authorities claiming that he had shot his father in the head and was holding the rest of his family hostage whilst planning on killing himself and his hostages by setting fire to the property. Tyler Barriss then proceeded to give the 9-1-1 operator Andrew Finch's address hoping that the police would respond whilst he was watching the victim via the internet (Koerner, 2018). Oddly, Tyler Barriss contacted the police in Wichita three times via phone that night and this should have raised alarm bells with law enforcement because none of the calls were direct to 9-1-1. Instead, Tyler Barriss attempted to mask his real identity by calling Wichita City Hall and then asking to be transferred to 9-1-1, thus covering his out of state telephone number with a local one and obfuscating the fact that he was 1,400 miles away from the alleged incident (Carrico, 2018).

Such masking behaviour is common amongst hoax callers to the police who utilise such methods in order to avoid prosecution for wasting police time. Had the police realised

that the call did not originate locally, then they may have treated it as hoax or carried out some more in-depth checks before they tasked units to respond. However, this masking activity was not detected and an alert was issued to all patrol units to respond in order to attempt to save the lives of the hostages in what was thought to be a time critical event. This led to the nearest patrol unit arriving at the address which had been given and taking control rather than the specially trained officers of a SWAT unit that may have been expected (Leiker & Potter, 2018). Having officers not specifically trained in how to deal with such a situation highly likely contributed to Andrew Finch's death as there were several further discrepancies which could have helped to end the situation peacefully. First, after the patrol officers arrived at the scene of the supposed crime, Taylor Barriss was actually on the phone with the police dispatchers for over 16 minutes, yet no attempt was made to confirm that he was physically present (Burgess, 2018). Also, the physical description which had been given of the property did not match that of Andrew Finch's real life dwelling and, whilst unclear, it appears that the patrol officers did not know that the dispatchers were in contact with the supposed suspect (Burgess, 2018).

Not being specifically trained in hostage situations, the patrol officers were unaware that these things should have been checked (Leiker & Potter, 2018), and thus when Andrew Finch stepped outside his home in order to see what all the police were doing in the area, he was killed by a single gunshot to the chest. The officer who fired the shot did so because he believed that Andrew Finch was reaching for a weapon and posed an immediate threat to life (Koerner, 2018); the Police Department in question concurred with the officer's assessment of the situation and no charges have been bought against him for shooting Andrew Finch (Manna, 2018). It was only during the investigation into Andrew Finch's death that the

police realised that he had been the victim of a 'swatting prank' and started to investigate further. Once they did so, the police quickly traced the 9-1-1 calls which had reported the original fake crime and 25-year-old Taylor Barriss was arrested. In an attempt to deter future instances of swatting, Taylor Barriss was charged with having carried out an act of domestic terrorism and was sentenced to 20 years in prison (Madani, 2018).

The above example becomes even more tragic when one becomes aware that Andrew Finch was not the intended target of this swatting incident. The original dispute over *Call of Duty: WWII* (Sledgehammer Games, 2017) had actually taken place between two online gamers – Casey Viner and Shane Gaskill. The pair took to *Twitter* in order to conduct their argument in public and during the argument Casey Viner threatened to kill Shane Gaskill (Madani, 2018). Casey Viner then contacted Taylor Barriss and provided an address that Shane Gaskill had claimed was his, but which was just one he picked at random which turned out to be that of Andrew Finch (Manna, 2018). Casey Viner received a 2-year community sentence, and, at the time of writing, Shane Gaskill is still awaiting sentencing (Leiker & Potter, 2018). The fact that an act of online braggadocio could lead to such a tragedy is something which should not have happened and that it did allows us to explore several structural deficiencies present in policing in the United States.

Swatting has been recognised as an act of online deviance since at least 2008 when the Federal Bureau of Investigation (FBI) issued a memorandum to police forces across the USA warning of the rising trend of these crimes (FBI, 2016). Despite such warnings, both the legal and policing response have been largely nonexistent with many states not possessing relevant legislation (Jaffe, 2016) and many police officers not being aware of the phenomenon (Jaffe, 2016). Andrew Finch's

case proves that such a lack of awareness has lethal consequences because it compounds the issue of self-defence immunity laws which exist, in most states, to protect law enforcement from prosecution for events that happen whilst they are carrying out their appointed duty (*Graham V. Connor*, 1989). Specifically, these laws often allow officers who have been involved in deadly shootings to avoid prosecution because they believed that the discharging of their weapon was justifiable as an act of self-defence, an act in defence of colleague or an act in defence of the public (*Graham V. Connor*, 1989). In practice, such legal protection gives US law enforcement officers a huge level of discretion as to when they are legally allowed to discharge their firearms. Effectively, this creates a policing model whereby suspicion that a violent act may be about to take place can lead to immediate use of lethal force by the police. The decision about whether or not a situation is violent is wholly subjective with the police officer involved making the decision based upon their perception of events.

For example, in the shooting of Andrew Finch, the officer who took the shot, Patrolman Justin Rapp of the Wichita Police Department, took approximately 10 seconds from seeing Andrew Finch on the front porch to opening fire (Koerner, 2018). Since the shooting took place, Officer Rapp has given two differing accounts of why he opened fire with his immediate statement claiming he saw a hand gun in Andrew Finch's hand (Madani, 2018) and his testimony in the court case of Taylor Barriss stating that he only believed that Andrew Finch was reaching for a hand gun concealed at his waistband (Koerner, 2018). As the officer responsible for shooting Andrew Finch was not charged and has been cleared of any wrong doing (Madani, 2018), those studying this and other fatal police shootings must ask questions about how they came to be normalised. A potential answer

lies in exploring the creation of SWAT teams in more depth. As mentioned previously, SWAT teams were explicitly created to handle criminal threats to which normal patrol officers do not have the equipment or training to handle. Whilst pragmatically this sounds like a solution to a problem in a gun culture, like that present in the United States, it also comes with several issues. As Kraska (2007) argues, the largest of these issues is the militarisation that SWAT teams bring into policing and how they blur the traditional dichotomous line between military and civil actions. Such a blurring takes place not necessarily amongst SWAT members who, research shows (Kraska, 2007), understand that they are modelled after elite military Special Forces units and are not actually engaged in similar actions but instead amongst those officers who aspire to be SWAT. Thus, a situation arises whereby patrol officers potentially come to see themselves as frontline troops engaged in a war against crime. If one conceptualises their role as a police officer in such a way, then those accused of crimes become the enemy and all police/suspect interactions become inherently adversarial as they are thought of as being a battle between the forces of law and order and those of criminality.

In such a context, academic research (Kraska, 2007; Waddington, 1993) has shown the likelihood of physical violence increases as the police officers start to consider themselves engaged in battle with mortal enemies who wish to kill them, their colleagues or members of the public. Such a potential cultural view amongst paramilitary style police units is compounded by the nature of the hoax situations which are called in by those attempting to have somebody swatted. As mentioned earlier, these hoax crimes are specifically invented to be as heinous as possible and often include accounts of multiple gruesome murders having already been carried out by the individual who is to be swatted. Being

tasked to respond to such an event, it is not hard to imagine the officers, who may already see themselves as engaged in battle, would arrive in a vengeful mood determined to stop the alleged offender from hurting any more innocents. So, whilst the lack of knowledge and training in this phenomenon contributed to the death of Andrew Finch, these deficiencies also speak to a wider difficulty, faced by law enforcement, in understanding how the virtual actions of individuals can carry over into analogue reality. Conversely, the ability to transcend the virtual and manifest in the analogue by exploiting the vengefulness that the police may feel is clearly very well understood by those who use online platforms to make a living with swatting being explicitly referred to as a means of punishing behaviour which oversteps the boundaries accepted by the online community. For example, one online gamer gave an interview about swatting where they described it as a means of physically controlling online behaviours:

> *When you're on the internet and your actions have little weight in real life, and then suddenly that translates into something as physically heavy as a swatting, it makes you realize the weight of your actions on a computer a lot more than you normally would. It did re-establish boundaries on the internet for them and remind them that just because they were behind a computer talking shit, it didn't mean they were untouchable.*
>
> (Koerner, 2018).

If we accept the above statement and consider it from a wider sociological viewpoint, we can understand the decision-making process behind swatting as being an attempt to police behaviours and interactions between online community members. In much the same way that family's police the

behaviour of small children by imposing physical punishments, such as groundings or timeouts, it appears that the online gaming community has developed methods for policing the Wild West (Allweiss, 1999), which is the internet. The Wild West analogy has been used to describe social interaction online due to the ease in which abusive behaviour which would not be tolerated in real life can be directed at people without any apparent consequence due to the anonymity afforded by usernames and avatars (Allweiss, 1999). At its most extreme, this abusive behaviour becomes known as trolling which consists of the specific targeting of people with very extreme abusive behaviour (Bishop, 2013). Often co-ordinated amongst a set of trolls, trolling is explicitly designed to cause harm to the victim with many trolls expressing enjoyment at the idea that their posts have led to physical or psychological harm having been caused (Bishop, 2013).

Such behaviour is destructive and can create highly toxic environments which spiral away from the topic which they were originally created to be about (Goodwin, 1994). However, the ability for the other members of the online community to do anything about a troll problem is traditionally nearly impossible. The anonymity they allow and ease with which new usernames can be created means that the banning of members from online communities does very little to limit troll behaviour (Bishop, 2013). In turn, this leaves online communities vulnerable and unable to do much more than either accept trolls as part of the virtual experience or for the nontroll members to migrate away to other platforms or service providers. This migration often cause a fragmentation of the online community with not all members successfully moving and it also does not limit the effect of trolls as they are often able to locate the users they are targeting across multiple platforms as evidence by Taylor

Barriss, Casey Viner and Shane Gaskill starting their argument on *Twitch.Tv* and then moving to *Twitter* (Madani, 2018). Yet, swatting can be reimagined away from being a prank designed to humiliate and towards being a form of online social policing with the public humiliation of being confronted by armed police whilst visible over a social media feed being the equivalent of the tarring and feathering that was carried out in premodern communities to punish minor infractions (Emsley, 2010). Therefore, swatting can be thought of as a retributive form of social justice utilised by those members of online communities which believe that they have been unfairly victimised, either by trolls or by the actions of a community member leading to loss of status of money. Unlike the banning of usernames or other virtual punishments which could be handed out, swatting is an inherently physical phenomenon which has real-world consequences for the targeted individual. This means that when an act of swatting is carried out, the motivations may not be as simple as revenge, humour or to cause humiliation it may be motivated by a desire to police what is in effect a lawless online community.

In conclusion, this chapter has attempted to show that swatting is a multifaceted and nuanced phenomenon that can be carried out for a variety of reasons. The fact that the act of swatting can be motivated by such disparate ideas as humiliation and humour means that it is likely to remain a popular activity for online communities to engage in. When these varied motivations are combined with the inherent anonymity of online activity and the implicit harm that swatting can cause the victimised individual, it is hard to see a downward trend in its occurrence. Such a reduction in this phenomenon is only likely to take place if major changes are made to legislation and policing at both a state and federal level across the United States.

REFERENCES

Allweiss, D. (1999). Copyright infringement on the internet: Can the Wild, Wild West Be Tamed? *Touro Law Review*, *15* (3), 1005–1052.

Bishop, J. (2013). *Examining the concepts, issues and implications of internet trolling*. Hershey, PA: Information Service Reference.

Burgess, K. (2018). Gamers express outrage, sorrow over swatting call that led to fatal shooting. *The Wichita Eagle*. Retrieved from www.kansas.com/news/local/article192461389. Accessed on September 17, 2019.

Calabro, S. (2018). From the message board to the front door: Addressing the offline consequences of race and gender based doxxing and swatting. *Suffolk University Law Review*, *51*(1), 55–74.

Carrico, L. (2018). Abstract assassination: How police militarization has contributed to the rise of "Swatting", Honours Thesis, Eastern Kentucky University, Richmond, KY. Retrieved from https://encompass.eku.edu/honors_theses/596/. Accessed on September 17, 2019.

Copeland, C., Wallin, M., & Holt, T. (2019). Assessing the practices and products of darkweb firearm vendors. *Deviant Behavior*. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/01639625.2019.1596465. Accessed on September 12, 2019.

Davidson, J., & Gottschalk, P. (2010). *Internet child abuse: Current research and policy*. London: Routledge.

Emsley, C. (2010). *Crime and society in England: 1750 – 1900*. Abingdon: Routledge.

Enzweiler, M. (2015). Swatting political discourse: A domestic terrorism threat. *Notre Dame Law Review*, *90*(5), 2001–2038.

FBI. (2008). Don't make the call: The new phenomenon of 'Swatting'. Retrieved from www.fbi.gov/news/stories/2008/february/swatting020408. Accessed on September 17, 2018.

FBI. (2016). The evolution of swatting. Retrieved from https://www.fbi.gov/audio-repository/news-podcasts-thisweek-the-evolution-of-swatting.mp3/view. Accessed on September 25, 2019.

Goodwin, M. (1994). Meme, counter-meme. Retrieved from https://www.wired.com/1994/10/godwin-if-2/. Accessed on September 25, 2019.

Graham V. Conor. (1989). Ruling by the United States Supreme Court, 490 U.S. 386.

Jaffe, E. (2016). Swatting the new cyberbullying frontier after Elonis V. United States. *Drake Law Review*, *64*(2), 455–484.

Katz, J., & Rice, R. (2002). *Social consequences of internet use: Access, involvement and interaction*. Cambridge, MA: Massachusetts University Press.

Koerner, B. (2018). It started as an online gaming prank. Then it turned deadly. Retrieved from www.wired.com/story/swatting-deadly-online-gaming-prank/. Accessed on September 17, 2018.

Kraska, P. (2007). Militarization and policing, it's relevance to 21st century police. *Policing*, *1*(4), 501–513.

Kraska, P., & Kappeler, V. (1997). Militarizing American police: The rise and normalization of paramilitary units. *Social Problems*, *44*(1), 1–18.

Leiker, A., & Potter, T. (2018). Tyler Barriss, gamers involved in fatal Wichita 'swatting' indicted on federal charges. *The Wichita Eagle*. Retrieved from www.kansas.com/news/local/crime/article211760059. Accessed on September 17, 2019.

Madani, D. (2018). Serial 'swatter' Tyler Barriss sentenced to 20 Years for death of Kansas man shot by police. Retrieved from https://www.nbcnews.com/news/us-news/serial-swatter-tyler-barriss-sentenced-20-years-death-kansas-man-n978291. Accessed on September 25, 2019.

Manna, N. (2018). Wichita police officer who fired fatal shot after swatting call won't face charges. *The Wichita Eagle*. Retrieved from www.kansas.com/news/local/crime/article208738719. Accessed on September 17, 2019.

Media Kix. (2017). Instagram influencer marketing is a $1.7 billion dollar industry. Retrieved from https://mediakix.com/blog/instagram-influencer-marketing-industry-size-how- big/#gs.11iq8q. Accessed on August 12, 2019.

Merriam-Webster. (2020). prank. *Merriam-Webster Online Dictionary*. Retrieved from https://www.merriam-webster.com/dictionary/prank. Accessed on March 16, 2020.

Radon, A. (2012). Counterfeit luxury goods online: An investigation of consumer perceptions. *International Journal of Marketing Studies*, *4*(2), 74–79.

Sledgehammer games. (2017). Call of Duty: World War 2. Foster City, CA: Sledgehammer games.

Spitz, M. (2010). Jackass: An oral history. Retrieved from https://www.maxim.com/entertainment/jackass-oral-history. Accessed on August 12, 2019.

Statt, N. (2017). Swatting over Call of Duty game results in deadly police shooting of Kansas man. Retrieved from www.theverge.com/2017/12/29/16830626/call-of-duty-swatting-prank-kansas-man-dead-police-shooting. Accessed on September 17, 2019.

Taylor, T. (2018). *Watch me play: Twitch the rise of game live streaming*. Princeton, NJ: Princeton University Press.

Twtich.tv. (2019). Don't just watch, join in, Retrieved from https://www.twitch.tv/p/about. Accessed on August 12, 2019.

Van Hout, M., & Bingham, T. (2013). 'Silk road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy*, *24*(5), 385–391.

Waddington, P. (1987). Towards paramilitarism? Dilemmas in policing civil disorder. *British Journal of Criminology*, *27*(1), 37–46.

Waddington, P. (1993). The case against police paramilitarism considered. *British Journal of Criminology*, *33*(3), 353–373.