Police behaving badly

Alice Hutchings
Director, Cambridge Cybercrime Centre
Department of Computer Science & Technology
University of Cambridge
Cambridge, UK
alice.hutchings@cl.cam.ac.uk

***Abstract*—Police officers and employees misusing access to police database now account for over half of all cybercrime prosecutions in the UK. The harms this can cause are considerable. Yet police continue to call for encryption to be weakened to allow for greater access to communication data.**

***Index Terms*—Cybercrime, policing, unauthorised access**

Some of the stories I come across in my research resemble movie plots. An encrypted messaging network and modified device provider is used by those involved in the illicit drug trade, murderers, gang violence, and other crimes for secure communication. A top secret law enforcement operation infiltrates the messaging service, leading to a huge amount of police intelligence and successful prosecutions. Less than six months into the infiltration, a corrupt UK police intelligence analyst working on a related case tips off a drug dealer friend that the messaging service is compromised. Shortly after, the service announces it is ceasing operations, disrupting countless active international police investigations.

Another story involves a love triangle, murder and intrigue. A protected witness gives evidence at the trial of a 'gangland execution', resulting in two convictions. One of the killers plans to appeal his conviction. Three months after the conviction, his girlfriend starts working for the police. Two months later, she makes her first attempt to unlawfully gather information from the police systems. However, she does not have access to the criminal intelligence system, which contain highly confidential information. She enlists the help of (and starts a relationship with) her colleague, who does have access. He makes numerous unauthorised attempts to discover the identity of the protected witness and others, and the information gathered is passed on to the killer's family.

I could envisage these movies starring Sandra Bullock as a plucky police officer, saving the day and restoring peace and harmony. Unfortunately however, they are egregious real-world examples of police staff behaving badly. The encrypted messaging service provider in the first example is EncroChat, and the infiltration was a joint operation of the French, Dutch, and UK authorities. The intelligence analyst later admitted misconduct in public office, perverting the course of justice and unauthorised access to computer material and was sentenced to three years and nine months in prison [1]. The second case resulted in the two lovers, employees of the Metropolitan Police, each receiving a five-year prison sentence [2].

These two examples are relatively high profile cases, embroiled in corruption, drugs, murder, and sex. They demonstrate the significant harms that can be caused, from the cost to witnesses, ongoing investigations, trust in the criminal justice system by the general public, and severing of trusted relationships with international authorities. Police employees have access to vast amounts of sensitive information, and this is vulnerable to misuse. This can include details of those who have had contact with the criminal justice systems, as witnesses, victims, suspects, and offenders.

Unfortunately, these examples are not isolated incidents. I maintain the Cambridge Computer Crime Database (CCCD) [3], a database of cybercrime events where the offender or alleged offender has been arrested, charged and/or prosecuted in the UK, dating from 1 January 2010. These are broadly classified as high tech offences, including those that fall under the Computer Misuse Act. The database also includes offences that involve the use of computers that fall under other legislation. This includes fraud, conspiracy, misconduct in public office, data protection, and money laundering offences where there is a link to high tech or cybercrime. The database is maintained by identifying relevant cases that are reported publicly in the news or police media releases.

In the UK, according to the CCCD, prosecutions involving police officers and staff made up the majority (56%) of finalised cybercrime-related court cases in the first half of 2024. The proportion of cases involving police as offenders is increasing, accounting for 47% of cases the last six months of 2023. In prior analyses of the CCCD, using data from 2010 to 2018, we found 23.5% of cases in the CCCD were alleged to occur within the workplace, and of these, 34.2% were believed to be committed by police officers and staff [4].

There are a number of explanations for this growing over-representation in the data. One is that internal abuse seems to be rife within police, perhaps enabled by a toxic police culture. Another explanation is that the majority of cybercrime never gets investigated or prosecuted, with offenders operating with impunity. Police offenders may simply be more visible and therefore account for the majority of prosecutions, which are not representative of the general offending landscape. The failure to prosecute other type of cybercrime seems to be amplified since the pandemic. The third explanation is more positive, which is that the police are detecting and prosecuting their own for misuse.

While police prosecuting their own for misuse to police databases is to be encouraged, it does then raise questions about where else misuse is occurring that does not reach public scrutiny. Internal misuse is not likely to be specific to police. Our previous analyses found some prosecutions involving bank employees, as well as the telecommunications and insurance industries, as well as the public sector, including health services (GPS, hospitals, and mental health service providers), and other public bodies (tax office, schools, and local authorities) [4]. However, these are unlikely to come anywhere near scratching the surface of internal misuse.

While the majority of police misuse will not be as scandalous as the first two examples, they still paint a disturbing picture [3]. Police employees have searched police databases to obtain sensitive data for disclosure to others, including organised crime groups. Much misuse highlights larger social problems, of toxic masculinity, power and control. Many cases involving men obtaining details of women for surveillance, stalking or spying. Their targets can include those they have come across during their police work, including young women who are vulnerable and in crisis. Other targets include current or former partners and others known to them. In some cases, the misuse of police databases has occurred alongside other offences, including the abuse of police powers. That is to say, the offences are not limited to what occurs in front of a computer screen. The implications are felt in real-world violence, sexual abuse, and coercion.

This misuse is occurring alongside longstanding law enforcement calls for greater access to citizens' communications data, the so-called 'cryptowars' [5]. Most recently, in the UK, the Online Safety Act 2023 includes provisions that would break end-to-end encryption to enable client side scanning. This is just one part of the law enforcement fight for weakening encryption to allow for police access [6]. As we have already seen, police have broken encryption used for communication by criminals (EncroChat), but the intelligence gained in this way does not necessarily stay with police for policing purposes, but can (and has been) be misused.

It is becoming clear that existing access policies and procedures in place within UK police forces are not working. Very strict access control measures are likely to introduce hindrances to police investigations, and unusable interventions will result in workarounds. In many cases, it is not obvious if police staff have searched for someone for legitimate purposes. They might be following a lead. Or perhaps they found someone attractive and wanted to know more about them. Or perhaps they found out who their ex was now dating. While in some cases police employees have misused access hundreds of times, in other cases it has only taken one instance for irreversible harm to have been caused.

What I fear is that police chiefs may decide the easiest way to address the problem is to do nothing, and sweep instances of misuse under the proverbial carpet. While this would lead to fewer prosecutions (and hence less public scrutiny), the lack of deterrence may lead to more widespread abuse. What is required is more than just technical access control solutions. Misuse is a social problem, and what also needs to be addressed is the toxic police culture and perceptions of impunity.

Overall, policing in the UK seems to be reaching a crisis point. There are countless stories of police abuses, including rape and murder, institutionalised racism, discrimination, corruption, and abuse of power. Historic abuses include undercover police deceiving women into deceptive intimate relationships. More recently, a Metropolitan Police officer received a life sentence for kidnapping, raping and murdering a young woman who had been walking home in the evening. These issues were recognised in the recent Independent Review into the standards of behaviour and internal culture of the Metropolitan Police Service, which concluded that the Met is 'institutionally sexist and misogynistic' [7]. What is missing from this somewhat damning report into the culture of the Metropolitan Police is any mention of misuse of their computer system, despite numerous prosecutions.

After 14 years of austerity during successive Tory governments, UK police have become woefully under-resourced [7]. They have nowhere near the capabilities to address the vast amounts of cybercrime that are experienced [8]. The new Labour government has committed to reducing crime. We will likely see much-needed resources for the police, but caution that more policing technologies will likely increase the means and motives for misuse if systemic issues are not also addressed.

In the UK, the Peelian Principles are the bedrock of policing. These principles are built on the idea that ethical policing happens by consent [9]. Public trust and confidence are crucial for the legitimacy of law enforcement. The more the police misuse their technological power, the less likely the public will trust them, requiring police to rely more on other forms of control or force to maintain order. Police should hold themselves to the same, or higher, standards of behaviour as the public they are protecting. Their use of computer systems should be in furtherance of a more trusting and peaceful society, not one where civilians are concerned about privacy or data abuse.

The level of prosecutions show those in public office can and do regularly abuse access to sensitive data. As our lives become more datafied, so do the opportunities for such data to be misused. This justifies the use, rather than the weakening, of end-to-end encryption.

BIOGRAPHY

I am Professor of Emergent Harms in the Security Group at the Computer Laboratory, University of Cambridge, and Fellow of King's College. I am also Director of the Cambridge Cybercrime Centre, an interdisciplinary initiative combining expertise from computer science, criminology, and law. Specialising in cybercrime, I bridge the gap between criminology and computer science. Generally, my research interests include understanding cybercrime offenders, cybercrime events, and the prevention and disruption of online crime.

ACKNOWLEDGMENT

This paper is part of a project that has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 949127).

I thank my colleagues at the Cambridge Cybercrime Centre, in particular Dr Ben Collier (University of Edinburgh) and Professor Alastair Beresford (University of Cambridge). While he did not get the chance to read this paper, it is inspired by the late Professor Ross Anderson, my friend and colleague and a formidable opponent in the cryptowars.

REFERENCES

[1] National Crime Agency, "Operation Venetic: Corrupt police worker jailed for tipping-off criminal over secret international investigation," https://perma.cc/ZXC2-T8DT.

[2] BBC News, "Woman jailed over plot to expose key witness in murder trial," https://perma.cc/475F-HSJV.

[3] Hutchings, Alice, "Cambridge Computer Crime Database," https://www.cl.cam.ac.uk/~ah793/cccd.html.

[4] A. Hutchings and B. Collier, "Inside out: Characterising cybercrimes committed inside and outside the workplace," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 481–490.

[5] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2008.

[6] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest *et al.*, "Bugs in our pockets: The risks of client-side scanning," *Journal of Cybersecurity*, vol. 10, no. 1, p. tyad020, 2024.

[7] Baroness Casey of Blackstock DBE CB, "Final report: An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service," https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/bcr/baroness-casey-review/, 2023.

[8] R. Anderson, C. Barton, R. Böhme, R. Clayton, C. Ganán, T. Grasso, M. Levi, T. Moore, and M. Vasek, "Measuring the changing cost of cybercrime," *Workshop on the Economics of Information Security (WEIS)*, 2019.

[9] J. Brown, *Policing in the UK*. House of Commons Library, UK Parliament, 2021.