Assignment 1:

# Drug Trafficking Cybermarkets and EncroChat:
# An Examination of the Legality of Cross-Judicial Evidence Sharing

*Transcript*

## Table of Contents

1. Table of Contents

Welcome to *Drug Trafficking Cybermarkets and Encrochat: An Examination of the Legality of Cross-judicial Evidence Sharing*. This presentation aims to discuss EncroChat, its judicial significance and connection to drug trafficking and policing in the UK, and the ramifications of its use as evidence as demonstrated by the appellant case *R v A, B, D & C [2021]* (Griffiths & Jackson, 2022). A legal debate regarding the case will be examined with a particular focus on forum shopping, along with public opinion. And finally, conclusions concerning possible legal concerns will be presented.

2. EncroChat

EncroChat was a mobile subscription service that offered anonymity to its client base. It did this through providing "communication between *Encro*-devices" (Stoykova, 2023: 1) with end-to-end encryption. This technology was beneficial to certain customers, as it made "decryption warrants or server access warrants useless." (Stoykova, 2023: 1). The devices themselves had no SIM card or connection to the customer, and offered a reasonable guarantee of no traceability. Moreover the devices reportedly had no camera, no microphone, GPS, or USB port and also came equipped with various methods for permanent data deletion (Zagaris, 2020), either through user command, maximum password entries, or remote execution through the EncroChat carrier help desk which operated 24 hours a day, seven days a week.

By 2020, EncroChat was the most popular telecommunication encryption service in Europe, not least for its ability to obfuscate organised criminal communication (Zagaris, 2020). But as illicit reputation grows, so too does the risk of law enforcement intervention (Davies, 2020). So

in 2017, the French Gendarmerie discovered that Encrochat was using French servers for operation and formed a joint investigation with Dutch law enforcement to create a technical device which could defeat EncroChat's encryption and surveil its customers (Zagaris, 2020).

Three years later in 2020, surveillance commenced for two months until, on 2 July, EncroChat became aware of the interception and dissolved while Europol, Eurojust, French, and Dutch authorities seized large amounts of evidence, and executed thousands of arrests across the EU and the UK for various crimes.

3. Drug Trafficking

A major example of one such offense in UK specifically was drug trafficking (Oerlemans & van Toor, 2022**)**. As technology has grown, so too has the traditional drug trade. While it is true that organised criminal groups comprise both traditional and cyber drug trafficking outfits, traditional drug trafficking is an inherently risky enterprise (Gori & Kabra, 2023). Gang rivalries over territory, supply, and delivery often leads to violence. While open-air territories themselves have a limited scope for demand, and expose group members to possible law enforcement investigation.

Organised criminal groups are "opportunistic economic agents" (Lavorgna, 2015: 156). Their entry into drug trafficking is often explained through Rational Choice Theory, wherein "individuals make decisions to engage in a particular criminal behaviour based on the rational weighing of the costs and benefits of that behviour" (Gori & Kabra, 2023: 3). The motivation of individuals to seek an increase in benefits and decrease in costs (Engeler & Bailetti, 2021) has at the same time spurred these groups to move their businesses into cybermarkets.

There are a number of benefits to doing so: use of the TOR browser (Munksgaard et al., 2016) ensures anonymity between the buyer and seller of the product. The risk of violence within these markets is zero. Advertising is simplified through 'surrogate advertising' and positive feedback on comment boards (Gori & Kabra, 2023). Distribution is widely expanded with "no need for wholesalers, brokers, traffickers, street sellers, or intermediaries" (Gori & Kabra, 2023: 2). Payment is safeguarded through the use of cryptocurrency and escrow accounts (Gori & Kabra, 2023), and PGP keys limit the ability of law enforcement to decrypt messages, even if they are found (Barrera et al., 2019). Use of encrypted communication devices such as Encrochat help facilitate the operation of groups within the cybermarket; members are able to communicate in real time without the constraint of computer access for anonymity. This adds to the overall cost/benefit ratio.

## 4. Policing in the UK

We will now look at policing in the UK as it relates to cybercrime. The first step to solving any cybermarket crime is identifying a suspect by locating their corresponding IP address (Holt et al., 2022). This is not possible when evaluating the IP addresses registered on a TOR network due to the use of server exit-nodes (Graham, 2 021), but there are several modes of investigation open to police which may result in a similar outcome.

They can interrogate acquired data, such as spreadsheets, logbooks, or customer lists if these are found in open source content (Davies, 2020). They can triangulate TOR exit-node data to make an educated guess concerning which websites a suspect has visited (Graham, 2021). They can trace public cryptocurrency transaction keys to similarly arrive at the identity of those involved in illegal transactions (Graham, 2021). They can go undercover as administrators on

websites, and, if necessary, they can use hacking tools to decrypt any information found from the above (Davies, 2020).

While all of these forms of investigation are possible, different legal jurisdictions allow for different policing abilities. For example, the UK does not allow an undercover investigator to commit crimes as part of his cover while the Queensland Police in Australia do. This has led to successful investigatory cooperation concerning the apprehension of child sexual abuse material in the past (Davies, 2020). Likewise the scope of tools accessible to hack a dark web application often differ depending on the scope of investigatory powers available (Stoykova, 2023). To circumvent these restrictions, Art. 21 of the Budapest Convention on Cybercrime allows law enforcement agencies to coordinate with other agencies who have the jurisdictional reach they lack (COE, 2001). The remainder of this presentation will discuss the legal implications of this practice as it relates to EncroChat and the UK legal system.

5. *R v A, B, D, C [2021]*

*The Crown v A, B, D & C* involve the appeal of four specific rulings made by Mister Justice Dove in regards to the admissibility of EncroChat evidence which aided the arrest and prosecution of the appellants (Griffiths & Jackson, 2022). For the purposes of this discussion, the first two shall be looked in detail as they encompass the fundamental arguments that inspire Grounds 3 and 4.

The first ruling, which states that "EncroChat communications were intercepted whilst being stored, not when being transmitted, thereby making them admissible" (Griffiths & Jackson, 2022: 272) was made due to the use of RAM storage for interception. The appellants argued that this ruling contradicts s.99(6) and s.3(1) of the Investigatory Powers Act (2016a & 2016b). S. 99(6)

ensures that interference must only be undertaken on stored communication according to guidelines of s.3(1) (IPA, 2016a).

S. 3(1) for its part states that unstored interception is an offence if committed within the realm of the United Kingdom (IPA, 2016b). Justice Dove found that the Targeted Equipment Interface warrants issued under s. 99 involved the EncroChat device RAM components, “part of the telecommunication system” (Griffiths & Jackson, 2022: 272), the data from which was technically stored on the device and not in transit at the time of interception. In addition the interception was not conducted in the UK, but rather in France. The appellant court upheld Justice Dove’s ruling and “rendered consideration of Ground 2 unnecessary” (Griffiths & Jackson, 2022: 272) based on Ground 1 findings, as it was redundant.

## 6. Legal Debate

Ground 2 is interesting in its logic, though, stating “[i]n the alternative [to Ground 1, i.e. if Ground 1’s terms are not met], no offence was committed under s.3 Investigatory Powers Act 2016 (IPA) as the interception was not done in the UK so could not be excluded by s.56 of the Act.” (Griffiths & Jackson, 2022: 272) With the permissiveness of transfer between Ground 1 and Ground 2, the Eurochat admissibility ruling may open a precedent that could be described as evidence forum shopping (Gori & Kabra, 2023; Griffiths & Jackson, 2022).

Legal debate concerning this tends to be focused on the problems of admissibility and fairness of trial. Fairness of trial proceedings concerning evidence in the UK is determined by s.78(1) of the PACE act of 1984 (PACE, 1984). The act makes clear that evidence can be excluded if “the circumstance in which the evidence was obtained [...] would have such an adverse effect on

the fairness of the proceedings" (PACE, 1984). Several factors from the EuroChat investigation support possible admissibility issues which could jeopardize the fairness of a trial based on such evidence.

Firstly, between "the United Kingdom and France, compared to domestic surveillance, there is no safeguard banning the collection and access to communications content" (Stoykova, 2023: 10). The French courts, which have interception powers "*extrema ratio* where other investigative methods would be unsuccessful or unavailable" (Galli, 2016: 667; Stoykova, 2023), relegated the investigation under military jurisdiction, and therefore under "national security exemption" (Stoykova, 2023: 11). As a result, it is impossible to know the true scope of the surveillance undertaken, nor how the privacy concerns of innocent users' communication was filtered by the the joint operation (Stoykova, 2023), as data stemmed from "mass surveillance that seems to lack specific purposes" (Stoykova, 2023: 11). At the same, "only the UK court came out with the conclusion that data in volatile [RAM] memory is stored, which is peculiar from both a legal and technical point of view" (Stoykova, 2023: 11). This raises uncomfortable concerns regarding the convenience of the ruling when considering the stipulations of IPA s.99(6) (2016a).

Additionally, France has no intention to appoint expert witnesses to explain the forensic data and processes that made up the investigation (Stoyakova, 2023). It is thus unclear how to the defense can properly "cross-examine the findings of the forensic examiner [to] identify the relevant data in the concrete investigation" (Stoyakova, 2023: 7). Importantly, though, the courts have used police officer testimony and hearsay concerning confidential reports in lieu of expert testimony, which does seem to violate s.78 of PACE (1984). It may place an undue burden of proof on the defense to disprove evidence that is impossible to verify (Skoykova, 2023).

Therefore, this privileged relationship between the UK and France, along with the unique RAM volatility rulings and lack of expert testimony or forensic analysis should factor greatly into what constitutes legal evidence admission among EncroChat cases to prevent unfair trial proceedings. That the UK has found in favor of EncroChat evidence admissions despite the above may indicate that UK courts are in violation of s.78 of PACE (1984) and s.99(6) of IPA (2016a), though this has yet to be the case.

## 7. Public Opinion

Public opinion of the EncroChat arrests are mixed-to-positive. There is a limited source of forums on UK newspaper websites, but commenters on *The Register* (Jellied Eel, 2023) seemed apprehensive of politicians redefining legal surveillance in the wake of the investigation, while those on *Echo* (Panther324, 2023) were in enthusiastic support. Neither shows the immediacy of the legal debate, which may reflect actual support, lack of knowledge, or lack of interest.

## 8. Conclusions

There are a number of considerations to be made concerning the EncroChat case data. Firstly, it is clear that cybercrime has proliferated on the dark web and that police investigation efficacy is limited by jurisdictional legislation restrictions. Though the EncroChat data technically satisfies the requirements of inclusion under s.3(1) of the IPA (2016b), serious doubts remain about its inclusion under s.99 of the IPA (2016a) and s.78 of PACE (1984). It is therefore pertinent to consider the evidence as presented when determining any admissibility under these acts. Each trial should have extensive evidentiary hearings regardless of the rulings of *R v A*, *B*, *D & C [2021]* until more concrete forensic evidence and expert witness testimony is released. Thank you.

9. References


Barrera, V., Malm, A., Decary-Hetu, D., & Munksgaard, R. (2019) Size and Scope of the Tobacco Trade on the Darkweb. *Global Crime*, 20 (1): 26 – 44

COE (2001) Budapest Convention on Cybercrime. *European Treaty Series*, (185): 1 – 22 [Available Online] https://rm.coe.int/1680081561

Davies, G. (2020) Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers. Journal of Criminal Law, 84 (5): 407 – 426

Engeler, S.M. & Balietti, S. (2021) Cryptocurrencies, Rational Choice, and Organized Crime. Dissertation. [Available Online] https://www.stefanobalietti.com/teaching/blockchain-econ-radical-markets/files/reports/2021/Engeler_Crypto_Crime.pdf

Galli, F. (2016) The interception of communication in France and Italy – what relevance for the development of English law? *International Journal of Human Rights*, 20 (5): 666–683

Gori, S. & Kabra, S. (2023) Drug Trafficking on Cryptomarkets and the Role of Organized Crime Groups. Journal of Economic Criminology, 2: 1 – 8

Graham, D. G. (2021) *Ethical Hacking: A Hands-On Introduction to Breaking In*. San Francisco, USA: No Starch Press.

Griffiths, C. & Jackson, A. (2022) Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat. The Journal of Law, 86 (4): 271 – 276

Holt, T., Bossler, A. & Seigfried-Spellar, K. (2022) *Cybercrime and Digital Forensics*. New York: Routledge.

IPA (2016a) *s. 99(6) Warrants under this Part: general* | Investigatory Powers Act 2016. legislation.gov.uk [Available Online] *https://www.legislation.gov.uk/ukpga/2016/25/section/99/enacted*

IPA(2016b) *s. 3(1b) Offence of Unlawful Interception* | Investigatory Powers Act 2016. legilation.gov.uk [Available Online] https://www.legislation.gov.uk/ukpga/2016/25/section/3/enacted

Jellied Eel (2023) With Great Power Come Great Responsibility | UK Cops Score Legal Win in EncroChat Snooping Op. theregister.com [Available Online] https://forums.theregister.com/forum/all/2023/05/12/nca_encrochat_warrants/

Lavorgna, A (2015) Organized Crime Goes Online: Realities and Challenges. *Journal of Money Laundering Control*, 18 (2): 153 - 168

Munksgaard, R., Demant, J., & Branwen, G., 2016. A replication and methodological critique of the study “Evaluating drug trafficking on the Tor Network”. International Journal of Drug Policy, 35: 92–96

Oerlemans, J. J. & van Toor D. A. G. (2022) Legal Apects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law, and Criminal Justice*, 30: 309 - 328

PACE (1984) *s. 78(1) Exclusion of Unfair Evidence*| Police and Criminal Evidence Act 1984. legislation.giv.uk [Available Online] https://www.legislation.gov.uk/ukpga/1984/60/section/78

Panther324 (2023) Conversation | Evidence on Encrochat Gang ’So Overwhelming’ Their Only Choice was to Plead Guilty. liverpoolecho.co.uk [Available Online] https://www.liverpoolecho.co.uk/news/liverpool-news/evidence-encrochat-gang-so-overwhelming-27814413

Stoykova, R. (2023) Encrochat: The Hacker with a Warrant and Fair Trials? *Forensic Science International: Digital Investigation*, 46: 1 - 14

Zagaris, B. (2020) EU and Law Enforcement Dismantle Encrypted Network of Transnational Organized Crime. International Enforcement Law Reporter, 36 (7): 248