7: UNLAWFUL DATA ACCESS AND ABUSE OF METADATA FOR MASS PERSECUTION OF DISSIDENTS IN TURKEY: THE BYLOCK CASE

A. SEFA OZALP

Introduction

This chapter presents a critical case study of unlawful metadata access and retroactive criminalization of encryption to persecute perceived dissidents by focusing on ByLock prosecutions in Turkey. Although ByLock was a public and free encrypted mobile chat application, the Turkish government argues that ByLock was exclusively used by the members of the Gulen Movement (GM), which the Turkish government accuses of organizing the failed coup attempt against President Erdogan in 2016. Under post-coup measures, tens of thousands of alleged ByLock users have been arrested under GM probe and handed down heavy prison sentences on terrorism charges. This chapter aims to highlight the threat of 'bad data' practices, such as criminalization of encryption, unlawful data access and abuse of communications metadata to persecute perceived dissidents, by unpicking the Turkish state's claims and the evidence presented to courts by the Turkish state during the ByLock trials. By doing so, this chapter contributes to current metadata retention and lawful access debate by detailing material effects of metadata exploitation for political purposes by government authorities. This chapter contends that lessons learned from the ByLock case illustrate how critical 'Good Data' principles and the integrity of encrypted and secure communication channels are for democracies.

Digital communication technologies (DCTs) have altered the way we generate, share and receive information. For the most part, DCTs have made public and private communications faster, cheaper, and easier. Although these advancements have been beneficial for people in general, DCTs have introduced new threats to privacy and information security. As the Snowden leaks revealed, DCT infrastructures have enabled state actors to access 'bulk' digital communications data and increased the surveillance capabilities of state actors exponentially.[1] Dissidents, minority populations and activists have been disproportionally affected by the increased digital surveillance efforts of state actors.[2]

In the age of DCTs, many fundamental rights essential for a 'Good Democracy' - such as the freedom of expression, the freedom of political thought, the freedom of religion, the freedom of association, and the right to privacy - are dependent on having strong information security. Freedom of expression is defined as the 'freedom to hold opinions and to receive and impart

1 Lina Dencik, Arne Hintz, and Jonathan Cable, 'Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism,' *Big Data & Society* 3.2 (2016), DOI: https://doi.org/10.1177/f2053951716679678.

2 G Greenwald and R Gallagher, 'Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters' *The Intercept,* 2014, https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/.

information and ideas without interference by public authority and regardless of frontiers' in the Charter of Fundamental Rights of the European Union (CFR).[3] In order to have a 'Good Democracy', activists, dissidents, or people in general need to be able to communicate securely to enjoy the freedom 'to receive and impart information without interference by public authority'.[4] Therefore, 'Good Data' and counter-surveillance practices such as online anonymity and encryption tools are integral to having a 'Good Democracy'. Since encryption is an essential tool to secure DCTs from state surveillance, encrypted and secure communication platforms frequently come under the attack by states, citing national security concerns.[5] These attacks constitute 'bad data' practices because they involve attempts to pass backdoor legislation, unlawfully spying on dissidents, activists and NGOs such as Privacy International,[6] and the use of unlawfully acquired or manipulated (meta)data to prosecute and/or persecute government critics.

To illustrate the oppressive potentials of 'bad data' practices, I introduce a case study of mass persecution of perceived government critics over their alleged usage of an encrypted communication application called ByLock in Turkey. ByLock was a free and public chat application which was downloaded more than 500,000 times from the App Store and Google Play Store between April 2014 and March 2016,[7] when it was deactivated when its developers stopped paying for the servers hosting the app.[8] Turkish Intelligence Agency (in Turkish Millî Istihbarat Teşkilatı, henceforth MIT) claimed that ByLock was a secret communication tool for Gulen Movement (henceforth GM) members - a social movement that the Turkish government holds responsible for the failed coup against Erdogan in 2016. In the aftermath of the coup attempt, the Turkish government accused any individual with perceived links to GM of being 'terrorists' and started an unprecedented purge. Shortly after the coup attempt, Turkish media reported that the MIT had hacked ByLock's servers in Lithuania, in an attempt to uncover ByLock users, perceived to be Gulenists.[9] MIT further claimed that they had identified thousands of ByLock users via metadata provided by Internet Service Providers (ISPs) and Mobile Network Operators (MNOs). Although the number of individuals ensnared under the ByLock investigation has not been officially released, Freedom House reported that 'Tens of thousands of Turkish citizens have been arbitrarily detained for their alleged use of the encrypted communications app ByLock'.[10] Mass arrests based on alleged ByLock usage have attracted severe criticism outside Turkey. The UN Human Rights Council called ByLock prosecutions a 'criminalization

3 European Union, 'Charter of Fundamental Rights of the European Union,' 2012, 391-407, https://doi.org/10.1108/03090550310770974.

4 Ibid.

5 David Lyon, *Surveillance After Snowden*, Cambridge: Polity Press, 2015.

6 Privacy International, 'Press Release: UK Intelligence Agency Admits Unlawfully Spying on Privacy International | Privacy International,' 2018, https://privacyinternational.org/press-release/2283/press-release-uk-intelligence-agency-admits-unlawfully-spying-privacy.

7 Fox-IT, 'Expert Witness Report on ByLock Investigation', Delft, 2017, https://foxitsecurity.files.wordpress.com/2017/09/bylock-fox-it-expert-witness-report-english.pdf.

8 Yasir Gokce, 'The Bylock Fallacy: An In-Depth Analysis of the Bylock Investigations in Turkey,' *Digital Investigation* (March, 2018): 2, https://doi.org/10.1016/j.diin.2018.06.002.

9 Freedom House, 'Freedom on the Net 2017 Report,' 2017, 15, https://freedomhouse.org/sites/default/files/FOTN 2017_Turkey.pdf.

10 Ibid, 14.

of encryption', noting that the 'evidence presented [by Turkish authorities] is often ambiguous'.[11] Amnesty International (AI) criticized ByLock prosecutions by stating that 'possession of internationally available and widely downloaded application does not represent a criminal offence' and the 'Turkish Government's methods for identifying users are seriously flawed in general'.[12] Similarly, Privacy International condemned the ByLock prosecutions and called for the immediate release of those arrested solely for using ByLock.[13]

Drawing on Cohen's moral panic theory,[14] I conduct a critical analysis of the post-coup measures taken by the Turkish regime, especially focusing on evidence cited in ByLock prosecutions. I conclude that the abuse of metadata to punish political enemies is not necessarily limited to authoritarian governments such as Turkey, as metadata are retained globally. By doing so, I present a cautionary case study from Turkey, detailing material effects of metadata exploitation for political purposes by government authorities, which digital activists and scholars around the world can draw on in the metadata retention and lawful access debates.[15] I argue that the abuse of metadata and unscrupulous law-enforcement powers can be easily justified in 'moral panics' when 'a condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests'.[16] I further argue that, supranational human rights legislation may be ineffective to prevent state surveillance, privacy breaches and metadata abuse. Finally, I contend that lessons learned from the ByLock case illustrate the importance of the 'Good Data' practices and the integrity of DCTs for 'good democracy'.

Digital Communication Technologies, Metadata and State Access

Before the emergence of DCTs, mass communication and public information campaigns were conducted through pre-digital information sharing mechanisms (ISMs) such as print media, radio, and television. Because of the nation-state-led developments in the technological infrastructure they relied on, pre-digital ISMs were relatively easier to influence for states and the powerful.[17] With the emergence of the internet and the DCTs, some scholars and

11 UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on His Mission to Turkey' (A/HRC/35/22/Add.3, 2017), 14, http://www.refworld.org/docid/59394c904.html.

12 Amnesty International, 'BRIEFING: Prosecution Of 11 Human Rights Defenders,' 2017, 7, https://www.amnesty.org/download/Documents/EUR4473292017ENGLISH.pdf.

13 Privacy International, 'Encryption At The Centre Of Mass Arrests : One Year On From Turkey's Failed Coup,' Privacy International, 2017, https://medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9.

14 Stanley Cohen, *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, third edition, London/New York: Routledge, 2002.

15 Amory Starr et al, 'The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis', *Qualitative Sociology* 31.3 (2008): 251-70, DOI: https://doi.org/10.1007/s11133-008-9107-z. ; Lisa M. Austin, 'Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State,' *SSRN* (2014), DOI: https://doi.org/10.2139/ssrn.2524653.

16 Cohen, *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, 282:1.

17 Hannu Nieminen, 'Digital Divide and beyond: What Do We Know of Information and Communications Technology's Long-Term Social Effects? Some Uncomfortable Questions', *European Journal of Communication* 31.1 (2016): 19-32, DOI: https://doi.org/10.1177/0267323115614198.

activists argued that these new media provided an opportunity to overcome some of the above challenges. One of the primary arguments brought forward was that the internet provided a decentralized infrastructure that allowed active participation of individuals online, which, in turn had the potential to disturb the pre-digital ISMs.[18] When equipped with 'Good Data' principles, DCTs provided a window of opportunity for activists and dissidents to revolutionize public and private communications. For instance, during the Arab Spring protests, online social media networks served as 'a common medium for professional journalism and citizen journalism, and as a site of global information flow' which, allowed activists to overcome state blackout and 'facilitating the revolutions'.[19] The revolutionary aspect of DCTs led some to believe - perhaps naively - that DCTs could provide users with an opportunity to become anonymous and protected from intrusive state surveillance. Current political, legal, and academic debates, however, illustrates that this is not the case.

One of the primary debates around DCTs concerns the retention of metadata and risks to user privacy.[20] In the context of DCTs, metadata are information about communications that users leave behind while using DCTs. For instance, while contents of the visited webpages are data, IP access logs and timestamps stored by ISPs are metadata. All user activities on DCTs, such as phone conversations, search queries, emails, website visits, ad-clicks, social media activities, and peer-to-peer messages, generate metadata which can be logged and stored automatically. Riley called this perennial form of large scale (meta)data collection 'dataveillance'.[21] Metadata can be aggregated, analyzed and sold to third parties. Using metadata, users can be profiled based on their political leanings, ethnic background, and sexual orientation. Inferences drawn from (meta)data analyses can be used for anti-democratic purposes, such as election meddling, as observed in the Cambridge Analytica case.[22] Metadata expand the surveillance capacities of state actors by revealing personal information such as 'who', 'when', 'what (type of communication)', 'how', 'where' which, in turn, 'can provide very detailed information regarding an individual's beliefs, preferences and behaviour'.[23] In fact, in the *Big Brother Watch vs UK* ruling, the European Court of Human Rights (ECtHR) ruled that 'metadata can be just as intrusive as the interception of content'.[24] Considering nation states are actively trying to exploit DCTs using both legal and illegal means,[25] the ease of access to

18 Peter Ferdinand, 'The Internet, Democracy and Democratization', *Democratization* 7.1 (2000): 1-17, DOI: https://doi.org/10.1080/13510340008403642.

19 Gilad Lotan et al, 'The Arab Springl The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions,' *International Journal of Communication* 5 (2011): 1377.

20 Monique Mann et al., 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im) Balance in Australia,' *International Communication Gazette* (in press, 2018), DOI: https://doi.org/10.1177/1748048518757141.

21 Rita Raley, 'Dataveilance and Countervailance' in in L Gitelman, *Raw Data' Is an Oxymoron*, Cambridge MA: MIT Press, 2013.

22 CNBC, 'Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal,' 2018, https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

23 Nora Ni Loideain, 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era,' *Media and Communication* 3.2 (2015): 54, DOI: https://doi.org/10.17645/mac.v3i2.297.

24 M Milanovic, 'ECtHR Judgment in Big Brother Watch v. UK,' EJIL:Talk!, 2018, https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/.

25 Amnesty International, 'Encryption. A Matter of Human Rights,' 2016, http://www.amnestyusa.org/sites/

metadata can be especially dangerous for political activists, dissident groups and perceived political opponents, who are subject to disproportionate and intrusive state surveillance.[26]

To date, national and supranational legal mechanisms have failed to provide comprehensive privacy protection for individuals. Governments around the world increasingly pass new laws that require metadata retention based on the argument of public security, pre-empting crime and terrorism.[27] Even in the EU context, where mechanisms such as CFR, ECtHR and the Court of Justice of the European Union (CJEU) provide a supranational level of legal protection against human rights breaches,[28] it is hard to talk about sufficient legal protection against government efforts to breach user privacy. For instance, the UK Government passed the Data Retention and Investigatory Powers Act 2014 (DRIPA) which required DCT providers to retain indiscriminate metadata on the grounds of national security and crime prevention. Both the Divisional Court and the Court of Justice of the European Union (CJEU) held that DRIPA was incompatible with EU law.[29] In a subsequent joint case ruling, CJEU found that the mass collection and analysis of metadata would lead to the violation of Article 7 [Respect to private and family life] and Article 8 [Protection of personal data] of the CFR, 'which could be justified only by the objective of fighting serious crime'.[30] Even though privacy organizations and activists welcomed this ruling, the CJEU left it to Member States to define what constitutes serious crime, hence the ability to adjust the balance of privacy versus national security. Indeed, in December 2016, the UK government replaced DRIPA with the Investigatory Powers Act which replicated the problematic elements of the DRIPA i.e. requirement for metadata retention and broad access by government agencies, even on non-crime related grounds.

Moral Panics and the Abuse of Metadata

To understand the true risks of metadata retention, it is beneficial to look at cases where authoritarian regimes exploit communications metadata to target political enemies and to facilitate oppression of dissidents - this is the focus of my analysis. In most cases, oppression faced by dissidents is a perennial process. Historical oppression of Kurds by the Turkish state and successive governments from different political backgrounds is a prime example of the continual oppression observed by dissidents.[31] However, in some cases, new political opponents can become targets. The latter is better observed within moral panics emerging

default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

26 Marcus Michaelsen, 'Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State', *Globalizations* 15.2 (2018): 248-64, DOI: https://doi.org/10.1080/14747731.2016.1263078.

27 UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye,' *Human Rights Council* (A/HRC/29/32: UN Human Rights Council, 2015).

28 The EU General Data Protection Regulation (GDPR) is not included here - despite being the most recent and comprehensive legislation which aims to protect user privacy - since its effectiveness in practice remains to be seen.

29 Isabella Buono and Aaron Taylor, 'Mass Surveillance in the CJEU: Forging a European Consensus', *The Cambridge Law Journal* 76.2 (2017): 250-53, DOI: https://doi.org/doi:10.1017/S0008197317000526.

30 Ibid, 251.

31 William Gourlay, 'Oppression, Solidarity, Resistance: The Forging of Kurdish Identity in Turkey', *Ethnopolitics* 17.2 (2018): 130-46, DOI: https://doi.org/10.1080/17449057.2017.1339425.

in the aftermath of political upheavals.

Goode and Ben-Yehuda's attributional model provides a useful theoretical perspective for understanding moral panics.[32] They propose five defining 'elements of criteria' i.e. *concern, hostility, consensus, disproportion* and *volatility* for moral panics. Authoritarian regimes are adept at constructing and propagating a 'folk devil' narrative to rationalize the persecution of political enemies and dissidents. These oppressive efforts increase when moral panics emege. Folk-devil narratives, constructed by authoritarian regimes, take advantage of widespread public *concerns* 'over the behaviour of a certain group or category'.[33] *Concerns* may be latent in society or be *volatile* i.e. surfacing suddenly following political upheavals. An example of the latter would be socially disruptive incidents, such as terror attacks, which act as 'trigger events',[34] and result in a 'heightened level of concern over the behaviour of a certain group or category.[35] In the aftermath of trigger events, the public becomes susceptible to be influenced by constructed folk devil narratives and 'an increased level of *hostility*' towards targeted groups may be observed.[36] Actively propagating 'folk devil' narratives may result in partial or complete *consensus* that 'the threat is real, serious and caused by the wrongdoing group members and their behaviour' across society.[37] Once there is a *consensus* of *hostility* towards the folk devils, *disproportionate* social and official reactions may be observed. Furthermore, disproportionate reactions may become '*routinized* or *institutionalized*', [38] and lead to impulsive and reactionary changes in 'legislation, enforcement practices, informal interpersonal norms or practices for punishing transgressors'.[39] As a result, overreactions can even be more damaging than the original threat for the public.

Correspondingly, abuse of communications metadata to confer criminality upon political enemies and dissidents can be easily justified following trigger events. As UNHRC Special Rapporteur David Kaye warned, 'efforts to restrict encryption and anonymity also tend to be quick reactions to terrorism, even when the attackers themselves are not alleged to have used encryption or anonymity to plan or carry out an attack'.[40] Extra-judicial mass surveillance programs of intelligence agencies, which would have been scrutinized and criticized by the public in normal times,[41] can be introduced in order to identify so-called 'terrorists'. Regimes can abandon established legal procedures and human rights protections such as 'the burden

32 Erich Goode and Nachman Ben-Yehuda, *Moral Panics The Social Construction of Deviance*, second edition, Chichester: Wiley-Blackwell, 2009.

33 Ibid, 37.

34 R D King and G M Sutton, 'High Times for Hate Crime: Explaining the Temporal Clustering of Hate Motivated Offending,' *Criminology* 51 (2013), DOI: https://doi.org/10.1111/1745-9125.12022.

35 Goode and Ben-Yehuda, *Moral Panics The Social Construction of Deviance*, 37.

36 Ibid, 38.

37 Ibid.

38 Ibid, 41. Emphasis in original.

39 Ibid.

40 UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye,' 13.

41 The UNHRC Special Rapporteur highlights that it is critical to have a 'transparent public debate' over privacy restrictions and intrusions. See para 35 of the 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye.'

of proof' or 'right to a fair trial' in pursuit of punishing political enemies. The oppression of dissidents can be facilitated by metadata abuse for political purposes i.e. citing unlawfully accessed or unreliable communications metadata to confer guilt on dissidents. To illustrate the oppressive potentials of such metadata abuse, I will look at the reactions to the coup attempt in Turkey, and the mass ByLock prosecutions in the aftermath.

The Turkish Coup Attempt and the Subsequent Purge

On 15 July 2016, a rogue group in the Turkish military took to the streets to topple President Erdogan. The coup had little chance of success: only a marginally small fraction of the Turkish military was involved,[42] and there was very little public support. While over two hundred soldiers and civilians were killed during the clashes, no government official was apprehended. By the morning, those involved in the coup were arrested and the coup attempt was suppressed. President Erdogan and the ruling Justice and Development Party (henceforth AKP) ministers publicly announced that the coup was organized by the GM, a social and religious movement who were at odds with the AKP at the time.[43] Erdogan personally called the attempt a 'gift from the God (sic)' which would 'allow him to cleanse the army and the state of terrorists [i.e. perceived GM supporters]'.[44] On the other hand, Gulen publicly denied any connection to the coup attempt, and called for an international commission to investigate the attempt; further

42 The International Institute for Strategic Studies, 'Turkey: The Attempted Coup and Its Troubling Aftermath,' *Strategic Comments* 22.5 (2016): v-vii, DOI: https://doi.org/10.1080/13567888.2016.1217082.

43 Space precludes a lengthier explanation of the fallout between the GM and AKP, but a short summary is needed to provide context for the reader. Even before the coup attempt, the GM was under heavy state pressure in Turkey. Both AKP and GM are Islam-inspired organisations, but they have categorical differences in interpretation. While the AKP is a political party founded by Erdogan and his allies in 2001 which adheres to nationalism and political Islam, the GM is a civil society organisation founded in Turkey in the late 1960s by the now-US-based Islamic cleric Fethullah Gulen, which prefers a civil interpretation of Islam with an emphasis on education. In terms of supporters, AKP is the largest party in Turkey with half of the popular vote (roughly 23 out of 46 million), the official number of GM sympathisers is unknown but estimates put it around 200,000-300,000. The GM used to run more than 2000 education facilities such as primary schools, high schools, and universities in Turkey, all of which have been confiscated by the AKP government. The GM runs more than a thousand education facilities outside Turkey in more than 100 countries. Despite being on good terms for nearly a decade since the AKP first won plurality in the 2002 legislative elections, the GM and AKP started diverging after 2012 over political disagreements. AKP accused GM of infiltrating state organs and forming a 'parallel state' i.e. having too many influential followers in state positions. The GM dismissed this criticism by arguing this was natural given that it provided good education to pupils in its institutions. When prosecutors in Istanbul opened Turkey's largest corruption investigations to date in late 2013, incriminating an Iranian-Turkish gold trader Reza Zarrab and Erdogan's son along with four cabinet ministers and their sons with credible evidence, Erdogan called the corruption investigation a 'judicial coup' and publicly declared GM as 'public enemy number one'. Media organisations affiliated with the GM ran stories defending the corruption probes and individuals representing GM started criticising AKP government vocally. From this point on, GM started facing a crackdown in Turkey. Just months before July 2016, the GM was declared a terrorist organisation by authorities and individuals allegedly linked to the movement started being arrested on terrorism charges.

44 Marc Pierini, 'Turkey's Gift From God' *Carnegie Europe*, 2017, http://carnegieeurope.eu/strategiceurope/?fa=67826.

stating that if any of his sympathizers were involved, they would have violated his values.[45] The extent of GM-linked individuals' possible involvement in the coup attempt is beyond the scope of this chapter. However, it is clear that following the coup attempt, GM faced extreme stigmatization from Turkish society both inside and outside Turkey, [46] leading GM members to leave Turkey for other countries and seek safety abroad.[47]

In the immediate aftermath of the coup attempt, the AKP government launched an unprecedented purge against perceived Gulenists. One day after the coup attempt, more than 2700 judges were dismissed,[48] and many were later arrested.[49] Even though the coup attempt was suppressed within hours, AKP government declared a state of emergency (henceforth SoE) and derogated from European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights (ICCPR). The derogation notice listed derogations from 13 articles such as the right to liberty, security, fair trial, privacy, the humane treatment of detainees, and the right to remedy, the latter two of which cannot be subject to derogation under any circumstances, according to the UN Human Rights Committee.[50] Additionally, the SoE allowed the AKP government to pass decrees without parliamentary scrutiny. For instance, SoE decrees provided full financial, administrative and criminal impunity to state officials for their actions during the SoE, which resulted in frequent torture and ill-treatment of detainees,[51] mass arbitrary arrests, arbitrary dismissal of state employees, and the removal of due process.[52] Consequently, dismissals have extended to perceived critics from other political backgrounds such as leftists, human rights defenders and Kurdish politicians. According to the latest figures,[53] more than 170,000 civil servants, including academics, teachers, police and military officers have been dismissed from their jobs without due process,[54] with 142,874

45 Emre Celik, 'Fethullah Gülen: 'I Call For An International Investigation Into The Failed Putsch In Turkey' *Huffington Post,* 2016, https://www.huffingtonpost.com/emre-celik/fethullah-guelen-i-call-f_b_11480974.html.

46 David Tittensor, 'The Gülen Movement and Surviving in Exile: The Case of Australia', *Politics, Religion & Ideology* 19.1 (2018): 123-38, DOI: https://doi.org/10.1080/21567689.2018.1453272.

47 Liza Dumovich, 'Pious Creativity: Negotiating Hizmet in South America after July 2016', *Politics, Religion and Ideology* 19.1 (2018): 81-94, DOI: https://doi.org/10.1080/21567689.2018.1453267.

48 This number later climbed over 4200 which amounts to one third of the total judges and prosecutors in Turkey.

49 Harry Cockburn, 'Turkey Coup: 2,700 Judges Removed from Duty Following Failed Overthrow Attempt' *The Independent*, 2016, https://www.independent.co.uk/news/world/europe/turkey-coup-latest-news-erdogan-istanbul-judges-removed-from-duty-failed-government-overthrow-a7140661.html.

50 United Nations Human Rights Committee, 'International Covenant on Civil and Political Rights - General Comment No. 29', *Annual Review of Population Law* 44470.29 (2001): 8, DOI: https://doi.org/10.1007/978-1-4020-9160-5_533.

51 Human Rights Watch, 'A BLANK CHECK: Turkey's Post-Coup Suspension of Safeguards Against Torture', 2016, https://www.hrw.org/sites/default/files/report_pdf/turkey1016_web.pdf.

52 Erol Önderoglu, 'Turkey: State of Emergency State of Arbitrary', *Reporters Without Borders*, (September, 2016): 15, https://rsf.org/sites/default/files/turquie.etatdurgence.eng_.def_.pdf.

53 When I submitted the first draft of this chapter, the figures were 150,000 dismissed, 133,257 detained, 64,998 arrested. By the time I submitted the second draft, the figures increased to over 170,000 dismissed, 142,874 detained, 81,417 arrested. These figures alone should be enough to illustrate the severity and arbitrary nature of the purge.

54 Amnesty International, 'NO END IN SIGHT: Purged Public Sector Workers Denied a Future in Turkey,' 2017, https://www.amnesty.org/download/Documents/EUR4462722017ENGLISH.PDF.

people detained and 81,417 people arrested.[55] These negative legislative and judicial developments have been demonstrated to be disproportionate, in breach of Article 4(1) of ICCPR,[56] and have had an extremely negative impact on the rule of law and individual liberties in Turkey.

In parallel with the regressive judicial and legislative developments, exploiting public concern and social tensions in the aftermath of the failed coup attempt, pro-AKP media and influential AKP figures constructed a 'Gulenist' narrative: covert terrorists and plotters infiltrated into society and the state, trying to demolish the state from within. Anyone suspected of being a GM member, supporter or sympathizer is a traitor and a terrorist. In this context, any activities performed by GM-affiliated individuals, such as charity work, donations, working in GM-linked institutions, organizing religious meetings or even simply *communicating with each other* have been ostracized and criminalized. This was exacerbated by Erdogan's presidential pleas for spying on family members and friends who are suspected to be Gulenists and reporting them to authorities.[57] Drawing on moral panic theory, we can see that the coup attempt has acted as a trigger event and the GM have been effectively declared the folk devils -'a category of people who, presumably, engage in evil practices and are blamed for menacing a society's culture, way of life, and central values' in the aftermath.[58] AKP government took advantage of public *concern* in the aftermath of the coup attempt aimed to construct a narrative to achieve *consensus* of *hostility* against GM. This was followed by disproportionate social, legislative, and judicial reactions. In this *volatile* social and political environment, it was relatively easy for the AKP government to weaken the established legal norms and individual safeguards their political enemies. It is fair to argue that, rather than the coup attempt, it was the AKP government's exorbitant and vindictive reactions to the coup attempt which resulted in mass human rights breaches, the eradication of the rule of law and individual liberties in Turkey.

ByLock Prosecutions: Mass Arrest of Perceived Opponents on Terrorism Charges over Encrypted App Usage

ByLock prosecutions were built on inaccurate claims and proceeded with disrespect to established legal standards and individual protections. Shortly after the coup attempt, AKP-linked media outlets published stories that coup plotters and their supporters communicated over ByLock during the coup attempt.[59] However, this claim is false, as Fox-IT clearly illustrated that the Bylock.net domain was deactivated in March 2016, hence ByLock 'could not have been used in the period from April 2016 leading up to 15 July 2016'.[60] The Turkish gov-

55 Turkey Purge, 'Turkey Purge | Monitoring Human Rights Abuses in Turkey's Post-Coup Crackdown,' 2018, https://turkeypurge.com/.

56 Ignatius Yordan Nugraha, 'Human Rights Derogation during Coup Situations', *International Journal of Human Rights* 22.2 (2018): 194-206, DOI: https://doi.org/10.1080/13642987.2017.1359551.

57 Laura Pitel, 'Erdogan's Informers: Turkey's Descent into Fear and Betrayal,' *The Financial Times*, 2017, https://www.ft.com/content/6af8aaea-0906-11e7-97d1-5e720a26771b.

58 Goode and Ben-Yehuda, *Moral Panics The Social Construction of Deviance*, 2.

59 Haber7.com, 'Darbeciler ByLock'tan Bu Mesajı Gönderdi! [English: Putchists Sent This Message on Bylock],' 2016, http://www.haber7.com/guncel/haber/2144267-darbeciler-bylocktan-bu-mesaji-gonderdi.

60 Fox-IT, 'Expert Witness Report on ByLock Investigation,' 9.

ernment also claimed that MIT identified ByLock user lists using 'special cyber methods' i.e. hacking Baltic/Cherry Servers in Lithuania which were hosting the ByLock app.[61] This means that MIT's access to ByLock server data was unlawful and such unlawfully acquired data 'shall not be presented before a court' and 'shall not constitute a factual ground for a possible conviction' under Turkish criminal law.[62] Both Lithuanian authorities[63] and Baltic/Cherry Servers[64] declared that they neither received a legal request from nor shared data with Turkish authorities, confirming Gokce's unlawful access observation. This is especially egregious because the ByLock prosecutions, which led to the arrest of tens of thousands of perceived GM members, were built on communication (meta)data accessed unlawfully.

Once the ByLock prosecutions started, MIT submitted a 'ByLock technical report' to trial courts, and this report constituted the technical basis of ByLock prosecutions.[65] The MIT report claimed that ByLock: (1) offered strong cryptography; (2) was disguised as a global application (i.e. presenting itself deceptively as a global application while the aim was to provide GM with an intra-organizational communication app); (3) was aimed at security and anonymity; (4) used a self-signed certificate; (5) offered communication only suitable for a cell-structure (as ByLock did not ask for a phone number to register, MIT argued that ByLock users could only exchange ByLock contact details after initially meeting face-to-face); (6) was designed to prevent access in case of legal confiscation; (7) offered identity hiding features (such as an automatic self-destruct, using long passwords features); and thus, concluded that 'ByLock has been offered to the exclusive use of the 'FTÖ/PDY' members [Gulenists]'.[66] Citing this report amongst evidence, first instance courts sentenced thousands of alleged ByLock users on terrorism charges (over alleged links to GM), ranging from 6 to 15 years.[67] The court of cassation, which acts as the unifying court of appeals in criminal prosecutions in Turkey, approved the evidential status of the alleged ByLock usage,[68] permitting the collective punishment of alleged ByLock users based on dubious lists created by MIT.

Despite the grave consequences for alleged ByLock users, the MIT report was found to be biased, insubstantial and unreliable when scrutinized by the Dutch cyber security firm Fox-IT.[69]

---

61 Gokce, 'The Bylock Fallacy: An In-Depth Analysis of the Bylock Investigations in Turkey,' 2.

62 Gokce, 3.

63 EN.DELFI, 'Lithuania Didn't Provide Turkey with ByLock User Data - Lithuania - m.En.Delfi.Lt,' 2017, http://m.en.delfi.lt/lithuania/article.php?id=76099973.

64 Gokce, 'The Bylock Fallacy: An In-Depth Analysis of the Bylock Investigations in Turkey.'

65 Although this report was not released to the public, it was distributed widely on social media. Fox-IT released the MIT report along with their own condemning report unpicking the inconsistencies and even deliberate manipulations in the former. Readers can find the Turkish version of the MIT report here: https://foxitsecurity.files.wordpress.com/2017/09/bylock-mit-technical-report-turkish.pdf.

66 Fox-IT, 'Expert Witness Report on ByLock Investigation,' 20.

67 The relevant article is Turkish Penal Code 314/2. See https://www.legislationline.org/download/action/download/id/6453/file/Turkey_CC_2004_am2016_en.pdf, p. 104.

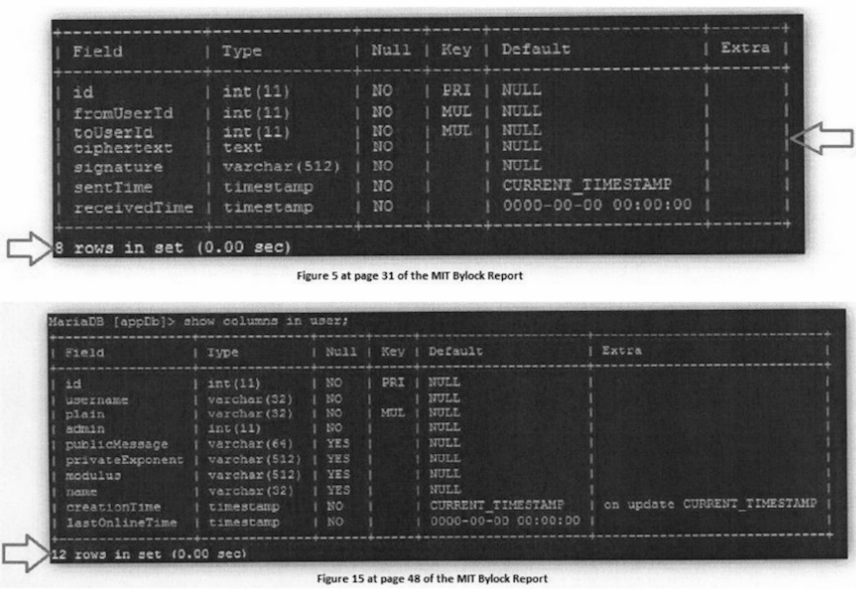
68 Reporters Without Borders, 'Journalists in New Wave of Arrests in Turkey,' 2017, https://rsf.org/en/news/journalists-new-wave-arrests-turkey.

69 Fox-IT illustrates tens of factual errors, irregularities, questionable and incorrect claims, and biased statements in MIT's technical report but space precludes the inclusion of all points illustrated. Fox-IT's report is so damning that it calls MIT's credibility in general into question.

By reverse engineering ByLock app's source code and online fact-checking, Fox-IT addressed claims put forward in the MIT report and found that: (1) 'security measures implemented in ByLock are not exceptional and actually on par with widely used chat applications';[70](2) the disguise of global application argument is 'not backed by evidence, questionable or incorrect';[71](3) ByLock developer's aim for security and anonymity 'does not imply an intent for use in illegal activities',[72] and 'in no way an indication that ByLock is aimed at a specific user group';[73](4) the incentive behind using a self-signed certificate is not necessarily to prevent authorities accessing the ByLock data, as self-signed certificates 'are easier to implement and are free of cost'; (5) rather than meeting face-to-face, users could have exchanged ByLock details using another communication method (e g. WhatsApp, Facebook, phone call), casting a shadow over MIT's 'ByLock was designed for communications in a cell structure argument'; (6) MIT is 'jumping to conclusions on the intent of the developer' when concluding ByLock was designed to 'prevent access in case of legal confusion';[74] and (7) measures such as self-destruct and using long passwords is a common feature also found in other communication applications such as Snapchat and Signal. As a result, Fox-IT concluded that MIT report is 'biased towards a predefined outcome', 'does not adhere to forensic principles', and is 'fundamentally flawed due to the contradicted and unfounded findings, lack of objectivity and lack of transparency'.[75]

MIT report also raised serious doubts about the integrity of data cited as evidence in ByLock prosecutions. Fox-IT noted that it is impossible to verify whether MIT tempered with ByLock server data or not because MIT did not calculate 'cryptographic hashes' of server data and did not 'generate an audit trail'.[76] Given that MIT is reported to have hacked ByLock servers, this is a crucial point that casts a great doubt over the evidential status of ByLock server data cited in prosecutions. In fact, screenshots used in the MIT report detailing the so-called investigation of the server data contain multiple inconsistencies 'that indicate manipulation of results and/or screenshots by MIT'.[77] In Figure 1, Gokce illustrates that the SQL query result screenshots presented in the MIT report (allegedly from data acquired from ByLock servers) are deliberately manipulated by MIT which 'points out the great likelihood that MIT and other Turkish authorities manipulated the Bylock database and fabricated false Bylock records'.[78]

70 Fox-IT, 'Expert Witness Report on ByLock Investigation,' 25.
71 Fox-IT, 20.
72 Fox-IT, 20.
73 Fox-IT, 25.
74 Fox-IT, 21.
75 Fox-IT, 28.
76 Fox-IT, 8.
77 Fox-IT, 29.
78 Gokce, 'The Bylock Fallacy: An In-Depth Analysis of the Bylock Investigations in Turkey,' 10.



Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
fromUserId	int(11)	NO	MUL	NULL	
toUserId	int(11)	NO	MUL	NULL	
ciphertext	text	NO		NULL	
signature	varchar(512)	NO		NULL	
sentTime	timestamp	NO		CURRENT_TIMESTAMP	
receivedTime	timestamp	NO		0000-00-00 00:00:00	

8 rows in set (0.00 sec)

Figure 5 at page 31 of the MIT Bylock Report

MariaDB [appDb]> show columns in user;

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
username	varchar(32)	NO		NULL	
plain	varchar(32)	NO	MUL	NULL	
admin	int(11)	NO		NULL	
publicMessage	varchar(64)	YES		NULL	
privateExponent	varchar(512)	YES		NULL	
modulus	varchar(512)	YES		NULL	
name	varchar(32)	YES		NULL	
creationTime	timestamp	NO		CURRENT_TIMESTAMP	on update CURRENT_TIMESTAMP
lastOnlineTime	timestamp	NO		0000-00-00 00:00:00	

12 rows in set (0.00 sec)

Figure 15 at page 48 of the MIT Bylock Report

Figure 1: Screenshots from MIT report, allegedly from ByLock database. Total numbers of rows returned by the SQL queries (7 and 10 respectively) do not match total numbers of rows shown at the bottom of the query results (8 and 12 respectively). Figure taken from Gokce (2018).

Although manipulation of evidence is a serious claim, Gokce makes a compelling argument that other not only MIT but also other Turkish authorities may also have 'fabricated' communications metadata (internet traffic records) to facilitate the sentencing of alleged ByLock users.[79] MIT report claimed ByLock users were identified by acquiring IP address logs from the ByLock server database, but it omits methods used to attribute these IP addresses to individuals. During criminal proceedings, it was revealed that the state relied on internet traffic metadata - namely IAL which contain information about date/time, public and private IP address of the user, target IP of the server connected amongst others - as evidence to identify individuals who communicated with ByLock's servers.[80] In Turkey, IAL are retained by the Information and Communication Technologies Authority (Bilgi Teknolojileri Kurumu in Turkish, henceforth BTK) which is the government institution authorized to collect and store metadata provided from ISPs and MNOs, which are private companies. In one scathing example of metadata fabrication, Gokce presents an alleged ByLock user's mobile IAL, which was exhibited to a criminal court during proceedings.[81] While the IAL produced by the MNO contains no data in the 'target IP' column for the specified time frame, the IAL produced by the BTK lists ByLock server's IP address in the 'target IP' column for the specified time

79 Gokce, 7.

80 The Arrested Lawyers Initiative, 'Ever-Changing Evidence ByLock: Turkish Government's Favourite Tool to Arrest Its Critics,' 2017, 14, https://arrestedlawyers.files.wordpress.com/2018/01/bylock_report_by_the_arrested_lawyers.pdf.

81 Gokce, 'The Bylock Fallacy: An In-Depth Analysis of the Bylock Investigations in Turkey,' 9.

frame. As BTK can only store metadata provided by MNOs and ISPs, one would expect no variation between IAL from BTK and MNO over the same time frame. Given this, the fact that only the IAL provided by BTK had 'target IP' information (i.e. IP addresses of servers hosting the ByLock app) indicates metadata manipulation and/or injection on BTK's side. This is a crucial point that lends support for Gokce's 'BTK doctored internet traffic records it received from telecommunication companies' argument.[82] These, coupled with the fact that Turkish authorities reduced the reported total number of ByLock users arbitrarily,[83] led critics to suggest that Turkish authorities have altered ByLock user lists arbitrarily to target perceived GM supporters. [84]

Even if we were to set aside claims of metadata manipulation, citing communications metadata as evidence in criminal prosecutions is unreliable because of IP-based attribution challenges. Without corroborating offline evidence, using IP addresses alone to identify individuals that are suspected for a crime is unreliable.[85] This issue is more frequently observed for mobile device IPs which connect to internet over a network provided by MNOs. Around the world, 92% of MNOs use Carrier Grade Network Address Translation (CGNAT),[86] which are network designs that distribute a small number of global IP addresses to many private users. This means, same public IP address can be shared by hundreds of users at a particular time, making it almost impossible to identify individual users via communications metadata. Indeed, EUROPOL reported that '90% of European cybercrime investigators regularly encounter attribution problems related to CGN technologies'.[87] Similarly, Turkish MNOs use CGNAT, which makes attempts to identify alleged ByLock users using communications metadata exceptionally error prone. In addition, individuals might have relied on 'Good Data' practices - such as using a VPN, a proxy server or Tor - to hide their IP addresses.[88] This makes attribution of ByLock usage based on communications metadata significantly unreliable. Furthermore, handing down lengthy prison sentences to individuals based on such unreliable metadata as evidence is likely to amount to a miscarriage of justice.

---

82 Gokce, 10.

83 The Arrested Lawyers Initiative, 'Ever-Changing Evidence ByLock: Turkish Government's Favourite Tool to Arrest Its Critics.'

84 Turkish Minister of Science and Technology first argued to have identified 215,000 ByLock users in September 2016. Then, in April 2017, AKP-linked media reported that the number of ByLock users had decreased to 102,000. In December 2017, Ankara Chief Prosecutor's Office announced over 11,000 misidentifications in ByLock lists, decreasing the final number to just over 90,000. Furthermore, the prosecution did not share digital data/evidence with defendants and their counsel. This led critics to suspect 'fabrication, alteration or corruption of the data' used in ByLock trials. See: The Arrested Lawyers Initiative report for an extensive summary.

85 Aaron Mackey, Seth Schoen, and Cindy Cohn, 'Unreliable Informants: IP Addresses, Digital Tips and Police Raids. How Police and Courts Are Misusing Unreliable IP Address Information and What They Can Do to Better Verify Electronic Tips', *Electronic Frontier Foundation*, 2016, https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf.

86 Philipp Richter et al, 'A Multi-Perspective Analysis of Carrier-Grade NAT Deployment,' *IMC '16 Proceedings of the 2016 Internet Measurement Conference*, 2016: 223, DOI: https://doi.org/10.1145/2987443.2987474.

87 Europol, 'IOCTA 2016: Internet Organised Crime Threat Assessment' (The Hague, 2016), 58, DOI: https://doi.org/10.2813/275589.

88 Mackey, Schoen, and Cohn, 'Unreliable Informants: IP Addresses, Digital Tips and Police Raids'.

In their report scrutinizing the Bylock prosecutions and the legality of actions of the Turkish state following the coup attempt, British criminal lawyers Clegg and Baker illustrated four significant breaches of the ECHR. First, alleged ByLock use does not satisfy the requirement of the ECHR Article 5:1(c)[reasonable suspicion of having committed and offence] and therefore, 'detention of persons on the basis that they had downloaded the Bylock App use is arbitrary and in breach of Article 5 of the convention [right to liberty and security]'.[89] Second, the MIT report is a clear breach of Article 6(3)(d) [right to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him], because 'authors of [the MIT] report are not identified' and 'no questions can be asked to the authors of the report'.[90] Third, mass dismissal and arrest of members of judiciary 'strikes at the heart of judicial independence and appears to be a further clear breach of Article 6 [the right to a fair trial]'.[91] Lastly, since both membership of GM and use of the ByLock app was legal before the coup attempt, to convict persons of membership of a terrorist organization on alleged ByLock use is 'clearly retrospective criminality and a clear breach of Article 7'.[92] The Turkish regime's breaches of the ECHR in the aftermath of the coup attempt - despite being a signatory of the ECHR - demonstrates that supranational human rights legislation may be ineffective to prevent metadata abuses by states. In the context of unlawful access and metadata retention debates, this means that 'broad mandatory [meta]data retention policies'[93] and 'A priori [meta] data retention or collection'[94] capabilities of states leave dissidents and political enemies of the states extremely vulnerable.

Lessons from the ByLock Case: Good Data Practices

In this chapter, by critically engaging with the ByLock prosecutions I detailed the material effects of metadata exploitation for political purposes outside of doctrinal analyses. This case study contributes to the metadata retention and lawful access debates, demonstrating both how existing capabilities of DCTs can be abused, and how extrajudicial - even illegal - investigative techniques can be introduced to oppress dissidents. Authoritarian governments like Turkey can and/or will take advantage of moral panics following political upheavals. 'Bad data' practices such as unlawful access and large-scale (meta)data retention and (meta)data manipulation can be instrumental to confer criminality on dissidents and political enemies, as observed in the ByLock case. Although regimes frequently spy on and surveil dissidents and

89 William Clegg and Simon Baker, 'Opinion on the Legality of the Actions of the Turkish State in the Aftermath of the Failed Coup Attempt in 2016 and the Reliance on Use of the Bylock App as Evidence of Membership of a Terrorist Organisation', London, 2017, 24, http://2oq5cg28288838bmfu32g94v-wpengine.netdna-ssl.com/wp-content/uploads/2017/09/Redacted-Opinion.pdf.

90 Clegg and Baker, 25.

91 Clegg and Baker, 26.

92 Clegg and Baker, 28.

93 UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye,' 19.

94 Amie Stepanovich and Drew Mitnick, 'Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance,' *Access Now*, 2015, 41, https://www.accessnow.org/cms/assets/uploads/archive/docs/Implementation_guide_-_July_10_print.pdf.

activists in normal times, moral panics certainly help regimes to justify unlawful, extrajudicial even illegal measures - such as criminalizing encryption usage - that would have been harder to implement in normal times.

Even though the scale and scope of mass arbitrary arrest of dissidents in the ByLock prosecutions are unprecedented, the threat of (meta)data abuse is not unique to dissidents in authoritarian regimes like Turkey. As metadata are being collected in 'bulk' globally, the very availability of metadata can be tempting for states to surveil dissidents, minority populations, activists, whistleblowers and government critics. On the other hand, although supranational human rights legislation and supranational judicial mechanisms have provided a degree of protection for human rights, their effectiveness in the face of oppression is questionable. Despite being a signatory of ECHR and a member of ECtHR, the Turkish regime has significantly breached the ECHR without facing any significant repercussions since the failed coup attempt. The mass human rights breaches observed in Turkey in the aftermath of the coup attempt call the credibility of supranational judicial mechanisms into question. Regimes can simply ignore or suspend the supranational judicial legislation citing perceived or even imagined national security concerns, as observed in the ByLock case. Given the possibility of the further rise of more authoritarian regimes in previously liberal countries, this case may be a grim precedent for things to come.

The ByLock case illustrates how critical 'Good Data' principles and the integrity of encrypted and secure communication channels are for 'Good Democracy'. In the age of DCTs, in order to exercise fundamental human rights - such as the freedom of speech, the freedom of political thought, the freedom of religion, and the freedom of association - strong and secure encrypted communications are essential. If we are not mindful and do not uphold, promote and defend 'Good Data' principles - whether they be more comprehensive and practical human rights legislation or technological solutions such as encrypted communications and anonymization tools - globally, regimes can and will compromise DCTs for 'bad' purposes, and the consequences for dissidents and governments critics are severe, as observed in the ByLock case. Therefore, we should remember that the ultimate promise of the 'Good Data' principles are not staying outside states' surveillance nets or communicating secretly; it is democracy itself.

References

Amnesty International. 'BRIEFING: Prosecution Of 11 Human Rights Defenders', 2017, https://www.amnesty.org/download/Documents/EUR4473292017ENGLISH.pdf.

_____. 'Encryption. A Matter of Human Rights', 2016, http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

_____. 'NO END IN SIGHT: Purged Public Sector Workers Denied a Future in Turkey', 2017, https://www.amnesty.org/download/Documents/EUR4462722017ENGLISH.PDF.

Austin, Lisa M. 'Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State.' *SSRN* (2014): 1-25, DOI: https://doi.org/10.2139/ssrn.2524653.

Buono, Isabella, and Aaron Taylor. 'Mass Surveillance in the CJEU: Forming a European Consensus', *The Cambridge Law Journal* 76.2 (2017): 250-53, DOI: https://doi.org/doi:10.1017/S0008197317000526.

Clegg, William, and Simon Baker. 'Opinion on the Legality of the Actions of the Turkish State in the Aftermath of the Failed Coup Attempt in 2016 and the Reliance on Use of the Bylock App as Evidence of Membership of a Terrorist Organisation.' London, 2017. http://2oq5cg28288838bm-fu32g94v-wpengine.netdna-ssl.com/wp-content/uploads/2017/09/Redacted-Opinion.pdf.

CNBC. 'Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal,' 2018, https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

Cockburn, Harry. 'Turkey Coup: 2,700 Judges Removed from Duty Following Failed Overthrow Attempt' *The Independent*, 2016. https://www.independent.co.uk/news/world/europe/turkey-coup-latest-news-erdogan-istanbul-judges-removed-from-duty-failed-government-overthrow-a7140661.html.

Cohen, Stanley. *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, third edition, London/New York: Routledge, 2002.

Dencik, Lina, Arne Hintz, and Jonathan Cable. 'Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism', *Big Data & Society* 3.2 (2016), DOI: https://doi.org/10.1177/2053951716679678.

Dumovich, Liza. 'Pious Creativity: Negotiating Hizmet in South America after July 2016', *Politics, Religion and Ideology* 19.1 (2018): 81-94, DOI: https://doi.org/10.1080/21567689.2018.1453267.

Emre Celik. 'Fethullah Gülen: 'I Call For An International Investigation Into The Failed Putsch In Turkey', *Huffington Post*, 2016. https://www.huffingtonpost.com/emre-celik/fethullah-guelen-i-call-f_b_11480974.html.

EN.DELFI. 'Lithuania Didn't Provide Turkey with ByLock User Data - Lithuania - m.En.Delfi.Lt,' 2017, http://m.en.delfi.lt/lithuania/article.php?id=76099973.

European Union. 'Charter of Fundamental Rights of the European Union,' 2012, 391-407, DOI: https://doi.org/10.1108/03090550310770974.

Europol. 'IOCTA 2016: Internet Organised Crime Threat Assessment', The Hague, 2016, DOI: https://doi.org/10.2813/275589.

Ferdinand, Peter. 'The Internet, Democracy and Democratization', *Democratization* 7.1 (2000): 1-17, DOI: https://doi.org/10.1080/13510340008403642.

Fox-IT. 'Expert Witness Report on ByLock Investigation.' Delft, 2017, https://foxitsecurity.files.wordpress.com/2017/09/bylock-fox-it-expert-witness-report-english.pdf.

Freedom House. 'Freedom on the Net 2017 Report,' 2017, https://freedomhouse.org/sites/default/files/FOTN 2017_Turkey.pdf.

Gokce, Yasir. 'The Bylock Fallacy: An In-Depth Analysis of the Bylock Investigations in Turkey', *Digital Investigation* (March, 2018): 1-11, DOI: https://doi.org/10.1016/j.diin.2018.06.002.

Goode, Erich, and Nachman Ben-Yehuda. *Moral Panics The Social Construction of Deviance*, second edition, Chichester: Wiley-Blackwell, 2009.

Gourlay, William. 'Oppression, Solidarity, Resistance: The Forging of Kurdish Identity in Turkey', *Ethnopolitics* 17.2 (2018): 130-46, DOI: https://doi.org/10.1080/17449057.2017.1339425.

Greenwald, G, and R Gallagher. 'Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters', *The Intercept*, 2014, https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/.

Haber7.com. 'Darbeciler ByLock'tan Bu Mesajı Gönderdi! [English: Putchists Sent This Message on Bylock]', 2016, http://www.haber7.com/guncel/haber/2144267-darbeciler-bylocktan-bu-mesaji-gonderdi.

Human Rights Watch. 'A BLANK CHECK: Turkey's Post-Coup Suspension of Safeguards Against Torture,' 2016, https://www.hrw.org/sites/default/files/report_pdf/turkey1016_web.pdf.

King, R D, and G M Sutton. 'High Times for Hate Crime: Explaining the Temporal Clustering of Hate Motivated Offending', *Criminology* 51 (2013), DOI: https://doi.org/10.1111/1745-9125.12022.

Laura Pitel. 'Erdogan's Informers: Turkey's Descent into Fear and Betrayal.' *The Financial Times*, 2017, https://www.ft.com/content/6af8aaea-0906-11e7-97d1-5e720a26771b.

Lotan, Gilad, Erhardt Graeff, Mike Ananny, Devin Gaffney, Ian Pearce and danah boyd. 'The Arab Spring | The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions', *International Journal of Communication* 5 (2011): 31.

Lyon, D. *Surveillance After Snowden*, Cambridge: Polity Press, 2015.

Mackey, Aaron, Seth Schoen and Cindy Cohn. 'Unreliable Informants: IP Addresses, Digital Tips and Police Raids. How Police and Courts Are Misusing Unreliable IP Address Information and What They Can Do to Better Verify Electronic Tips', *Electronic Frontier Foundation*, 2016, https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf.

Mann, Monique, Angela Daly, Michael Wilson and Nicolas Suzor. 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia', *International Communication Gazette* (in press, 2018): DOI: https://doi.org/10.1177/1748048518757141.

Marc Pierini. 'Turkey's Gift From God' *Carnegie Europe*, 2017, http://carnegieeurope.eu/strategiceurope/?fa=67826.

Michaelsen, Marcus.'Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State', *Globalizations* 15.2 (2018): 248-64, DOI: https://doi.org/10.1080/14747731.2016.1263078.

Milanovic, M. 'ECtHR Judgment in Big Brother Watch v. UK.' EJIL:Talk!, 2018, https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/.

Ni Loideain, Nora. 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era', *Media and Communication* 3.2 (2015): 53, DOI: https://doi.org/10.17645/mac.v3i2.297.

Nieminen, Hannu. 'Digital Divide and beyond: What Do We Know of Information and Communications Technology's Long-Term Social Effects? Some Uncomfortable Questions', *European Journal of Communication* 31.1 (2016): 19-32, DOI: https://doi.org/10.1177/0267323115614198.

Nugraha, Ignatius Yordan. 'Human Rights Derogation during Coup Situations', *International Journal of Human Rights* 22.2 (2018): 194-206, DOI: https://doi.org/10.1080/13642987.2017.1359551.

Önderoglu, Erol. 'Turkey: State of Emergency State of Arbitrary', *Reporters Without Borders* (September, 2016): 15, https://rsf.org/sites/default/files/turquie.etatdurgence.eng_.def_.pdf.

Privacy International. 'Encryption At The Centre Of Mass Arrests : One Year On From Turkey's Failed Coup.' *Privacy International*, 2017, https://medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9.

_____. 'Press Release: UK Intelligence Agency Admits Unlawfully Spying on Privacy International | Privacy International,' 2018, https://privacyinternational.org/press-release/2283/press-release-uk-intelligence-agency-admits-unlawfully-spying-privacy.

Raley, R. 'Dataveillance and Countervailance' in L Gitelman, *Raw Data' Is an Oxymoron*, Cambridge, MA: MIT Press, 2013.

Reporters Without Borders.'Journalists in New Wave of Arrests in Turkey', 2017. https://rsf.org/en/news/journalists-new-wave-arrests-turkey.

Richter, Philipp, Florian Wohlfart, Narseo Vallina-Rodriguez, Mark Allman, Randy Bush, Anja Feldmann, Christian Kreibich, Nicholas Weaver and Vern Paxson. 'A Multi-Perspective Analysis of

Carrier-Grade NAT Deployment', *IMC '16 Proceedings of the 2016 Internet Measurement Conference*, 2016, 215-29, DOI: https://doi.org/10.1145/2987443.2987474.

Starr, Amory, Luis A. Fernandez, Randall Amster, Lesley J. Wood,and Manuel J. Caro. 'The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis', *Qualitative Sociology* 31.3 (2008): 251-70, DOI: https://doi.org/10.1007/s11133-008-9107-z.

Stepanovich, Amie, and Drew Mitnick. 'Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance' *Access Now*, 2015, https://www.accessnow.org/cms/assets/uploads/archive/docs/Implementation_guide_-_July_10_print.pdf.

The Arrested Lawyers Initiative. 'Ever-Changing Evidence ByLock: Turkish Government's Favourite Tool to Arrest Its Critics', 2017, https://arrestedlawyers.files.wordpress.com/2018/01/bylock_report_by_the_arrested_lawyers.pdf.

The International Institute for Strategic Studies. 'Turkey: The Attempted Coup and Its Troubling Aftermath', *Strategic Comments* 22.5 (2016): v-vii, DOI: https://doi.org/10.1080/13567888.2016.1217082.

Tittensor, David. 'The Gülen Movement and Surviving in Exile: The Case of Australia', *Politics, Religion & Ideology* 19.1 (2018): 123-38, DOI: https://doi.org/10.1080/21567689.2018.1453272.

Turkey Purge. 'Turkey Purge | Monitoring Human Rights Abuses in Turkey's Post-Coup Crackdown', 2018, https://turkeypurge.com/.

UN Human Rights Council. 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye.' *Human Rights Council*. A/HRC/29/32: UN Human Rights Council, 2015.

_____. 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on His Mission to Turkey.' A/HRC/35/22/Add.3, 2017. http://www.refworld.org/docid/59394c904.html.

United Nations Human Rights Committee. 'International Covenant on Civil and Political Rights - General Comment No. 29.' *Annual Review of Population Law* 44470.29 (2001): 8, DOI: https://doi.org/10.1007/978-1-4020-9160-5_533.