Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk hack

Maria Grazia Porcedda, and David S. Wall[1]

Abstract— Big data and cybercrime are creating 'upstream', big data related cyber-dependent crimes such as data breaches. They are essential components in a cybercrime chain which forms a cybercrime ecosystem that cascades 'downstream' to give rise to further crimes, such as fraud, extortion, etc., where the data is subsequently monetized. These downstream crimes have a massive impact upon victims and data subjects. The upstream and downstream crimes are often committed by entirely different offending actors against different victim groups, which complicates and frustrates the reporting, recording, investigative and prosecution processes. Taken together the crime stream's cascade effect creates unprecedented societal challenges that need addressing in the face of the advances of AI and the IoT. This phenomenon is explored here by unpacking the TalkTalk case study to conceptualize how big data and cloud computing are creating cascading effects of disorganized, distributed and escalating data crime. As part of the larger CRITiCal project, the paper also hypothesizes key factors triggering the cascade effect and suggests a methodology to further investigate and understand it.

Index Terms— cybercrime, big data, big data crime, cloud computing, crime scripts, crime cascade.

I. Introduction: The ever-changing nature of cybercrime[2]

Cybercrime is an ever-changing and constantly evolving threat. In 2019, Symantec documented significant changes in attack vectors in 2018, for example a 63% fall in unique pieces of malware detected per year during the year (from 670m in 2017) contrasted with a dramatic increase in attacks that in one way or another target data such as web attacks (+56%), mobile ransomware (+33%) and supply chain attacks (+78%) plus formjacking[3] (no corresponding 2017 data) [41]**.** Although indicating a shift in offender priorities, this change reflects two predominant features in cybercrime over the past decade. The first is an appetite for gaining unauthorized access to data for financial or intelligence gain [17]. Europol, for example, found in their IOCTA report (p. 22) that over one third of Member States reported incidents relating to illegal acquisition of data [19] (p. 7). The illegal acquisition of data via data breaches not only disrupts businesses and organisations but also facilitates further criminal activity [19]. The second constant feature of cybercrime is the development of deepweb marketplaces selling stolen data and other stolen goods, as well as cybercrime-as-a-service [43][19][16].

The development of deepweb marketplaces has attracted considerable attention and led to discussions about the emergence of mafia type 'organized cybercrime' groups online [24][6][23]. This observation is disputed [44][22], as we discuss later in the paper, because it seems that different offending groups and unconnected individuals are simultaneously involved, although there is further research still to be done to look at the organised nature of groups operating in dark marketplaces [28]. Here we mainly focus upon big data crime (mainly Data Breaches, DDoS attacks and Spamming), which result from big data and cloud computing and are arguably the underlying causes of most modern cybercrime.

Today, Big Data is a massive industry whose potential for monetization attracts legitimate businesses and cybercriminal entrepreneurs alike. The paradigm of cloud computing makes increased connectivity and data processing possible, thereby supporting the flourishing of both big data and cybercrime. As we suggested in earlier articles [34] (p. 216), Big Data Crimes [47] are upstream and cyber-dependent [46] but 'cascade' crime downstream to enable cyber-enabled and even cyber-assisted cybercrimes [46]. This cascade is very hard to track and counter, but we hope to identify various tipping points where information and data cascade downwards to facilitate further crime. By catching actions at such tipping points, for example, the data dump or point of sale, then the subsequent 'crime frenzy' could in theory be prevented.

In this paper we seek to conceptualise the 'cascade effect' and in so doing, also identify key 'tipping points' upon which law enforcement action can be focused. To illustrate this process, we draw upon a case study of the data breach suffered by TalkTalk Telecom Group PLC (hereafter TalkTalk) in 2015 [5]. The discussion below refers to past events and relies on the TalkTalk case because so much information is available in the public domain which enables us to not only understand the processes of victimisation and the cascade, but also the response of the criminal justice system and incident prevention, whilst also helping us propose such attacks as 'ideal types' for

[1] Maria Grazia Porcedda, Centre for Criminal Justice Studies, School of Law, University of Leeds, (e-mail: m.g.porcedda@leeds.ac.uk).

David S. Wall, Centre for Criminal Justice Studies, School of Law, University of Leeds, (e-mail: d.s.wall@leeds.ac.uk).

[2] This paper was submitted for review on 22/2/2019. It is based upon work funded by the CRITiCal ('Combatting cRiminals In The Cloud' - EPSRC EP/M020576/1) and the EMPHASIS projects ('EconoMical, PsycHologicAl & Societal Impact of RanSomware' - EPSRC, EP/P011772/1).

[3] Formjacking (from mid-2018) improves the effectiveness of social engineering by using a type of Javascript-code injection to take over the functions of a website's form page to collect information about the user and send it back to the hacker.

future analysis. We should also point out that although this case caused TalkTalk major embarrassment and financial loss, significant security improvements have since been made and the company has recovered. Moreover, our use of this case is primarily illustrative and is not intended to claim casual inference [64].

II. Background to The TalkTalk Case

In October 2015, news outlets extensively covered a data breach suffered by TalkTalk, a UK based TV, broadband, mobile and phone provider [5][18][45]. The scale of the breach was such as to cause the launch of a parliamentary inquiry into cyber security and the protection of personal data online, published in June 2016 [14]. This breach is also significant because it was very well documented from inception to prosecution and the circumstances of the breach and (for researchers) the detection, arrest and prosecution of the offenders reveal in considerable detail the construction of a modern 'Big' cybercrime. More importantly, this case study, as indicated earlier, also reveals important information about the levels of interdependency within the modern cybercrime ecosystem and, where relevant, the division of labour within the offender group.

The TalkTalk breach exposed personal information contained in a database called 'Tiscali Master' accessible from webpages [18] that were inherited from Tiscali, which TalkTalk had acquired in 2009 via Carphone House.

In October 2015, hacker(s) using the alias "Fearful" and "Glubz" used the SQL map programme, an open source penetration testing tool "that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers"[4] to probe the webpages. "Glubz" found vulnerabilities in three of the old Tiscali webpages now owned by TalkTalk [18]. Krebs reports that "Glubz" posted the vulnerability in the videos section of TalkTalk's Web site[5] on October 18th [21], but that "Glubz" did not personally exploit the information [21].

The flaw was further reported on xssposed.org, which Krebs describes as a site that operates as a clearinghouse for unpatched vulnerabilities. It is not clear whether it was reported by "Glubz" or by Hanley (see below), or someone else. Xssposed.org verified that the flaw existed but did not release technical details to the public so that TalkTalk would have time to patch the vulnerability, thereby protecting its users [21].

Bisson [5] reported that Richard De Vere, Principal Consultant for the AntiSocial Engineer Ltd., contacted TalkTalk to inform them of a serious vulnerability on October 21st. The company did not act on these warnings at the time.

Later, on October 21st, the same day that De Vere had warned TalkTalk, Bisson [5] notes that DownDetector[6] recorded a spike in technical issues associated with TalkTalk. Customers had problems making calls or logging into their email until the ISP's website became completely unavailable. According to Krebs, the DDoS (denial-of-service attacks), which prevented legitimate users from accessing the website, were launched to distract TalkTalk security from the SQLi attack to hack the database [21]. The TalkTalk website was allegedly attacked over 14,000 times [11][18].

Bisson [5] found that, on October 23rd, Trista Harrison, Managing Director (Consumer) of TalkTalk, had posted an "update on the company's website" explaining that TalkTalk had suffered a "significant and sustained cyber-attack" two days before. Harrison explained that "the names, addresses, dates of birth, and credit card/bank details of as many as four million TalkTalk customers might have been compromised by the hack [5]. Furthermore, TalkTalk CEO Dido Harding confirmed TalkTalk received an email from a group alleging responsibility for the breach and requesting a ransom in return for not publishing or selling the data [5]. Eventually Harding also received several blackmail attempts [37].

According to Krebs, multiple hacker collectives claimed responsibility for the hack; the BBC even claimed one as a "Russian Islamist group". At the same time, "Courvoisier" (an identity later attributed to Grant West [36]), promised to post the stolen data on the now defunct deep web black market AlphaBay, which he promised would be in the following format [21]:

> Name; DOB; Address; TenancyType; YearsAtAddress; MonthsAtAddress; HomeTelephone; MobileTelephone; Email; Employer; EmploymentTitle; EmploymentLocation; EmployersPhone; Bank; AccountNumber; and SortCode.

According to Krebs, Courvoisier appeared to be a "Level 6 Fraud and Drugs seller," that is someone "who has successfully consummated at least 500 sales worth a total of at least $75,000 and achieved a 90% positive feedback rating or better from previous customers" [21]. Two weeks after the attack, it was reported that another AlphaBay user, with the nickname of 'Martian', was selling TalkTalk customers' breached financial data for £1.62 a time [42].

Bisson reports that, on October 24th, there were suggestions that hackers had exploited TalkTalk customers' credit card details and bank accounts. Among them, Hilary Foster, a barrister's clerk from southwest London, said she blocked her card after scammers stole cash from her bank account and used it to purchase £600 worth of goods. Another user had his broadband connection interfered with [5]. Another TalkTalk customer contacted The Register claiming to have lost £3,500 days after the breach [25].

In her update of October 23rd, Trista Harrison explained that Dido Harding, the chief executive of the company, urged "customers to be wary of unexpected phone calls that ask for personal information with respect to their TalkTalk accounts" [5]. Harding might have been wary of opportunistic scammers who may have accessed information about TalkTalk customers from dumped data and call breached victims at home to further defraud them. This was reported in a Channel 4 news program [7] which showed how a TalkTalk customer affected by the hack was subsequently scammed by two opportunistic young men based in India [9] who were not involved in the initial hack.

[4] SQLMAP - http://sqlmap.org/.

[5] TalkTalk Video Section - videos.talktalk.co.uk.

[6] DownDetector - https://downdetector.com/.

To be sure, such a scam is not specific to the October 2015 TalkTalk breach. On October 25th TalkTalk customer Mike Barrie told BBC News that, a few months back, he had received a fraudulent call from a self-expressed TalkTalk employee [2]. Upon reporting the incident, the company allegedly "didn't seem very interested." Mr Barrie believed TalkTalk might have already been hacked in the past [5], as the Information Commissioner's Office (ICO) would later confirm [39]. Actually, Ms Harding might have also been wary of another form of scam involving the abuse of personal data which came under the scrutiny of the ICO. Indeed, on top of the £400,000 fine for the 2015 breach (which was a very harsh penalty prior to the DPA 2018), TalkTalk also received a £100,000 fine by the ICO [57, 58], because employees based in the Wipro call centres in India misused data of TalkTalk customers in a scam where they posed as engineers offering to fix remotely an ostensible vulnerability on their computers. This is completely unrelated to the October 2015 data breach.

Simply put, scammers may have used known techniques to try to further target victims of the TalkTalk hack. Or, they may have tried to prey on victims. The Daily Mail's Sam Greenhill was also affected by the TalkTalk hack. He was the object of opportunistic calls by engineers posing as TalkTalk computer support personnel [13]. The people who contacted him did not refer to the hack, but instead offered to provide Windows-related support.

III. TALKTALK AND THE CASCADE EFFECT

The 'chain' of intrusion, a.k.a. the attack chain, is a recognized concept [17]. It refers to the fact that cybercrime requires offenders to successfully progress through a series of linked stages. For instance, data exfiltration requires accessing a system without authorization, which in turn presupposes several options, such as infecting websites, performing an SQL injection to assist removal of data, or sending an email containing an infected attachment. Proofpoint provide a very useful technical analysis of an attack chain in their Analysis of a Cybercrime Infrastructure [38][29]. They show systematically how a cybercrime group compromised PCs via a range of processes that included credential sniffing, uploading malware via compromised sites onto unprotected Windows XP machines. They then used those PCs to offer a sophisticated, paid proxying service to organized crime groups that turns infected PCs into an illicit 'private cloud', as well as infiltrating corporate networks [38]. What Proofpoint do not do is show how the individuals involved interacted with each other or establish the casual relationships which led to many big data cybercrimes, which is why the TalkTalk case is so important. Here we build on the notion of chain and cascade to propose tipping points at which the one cybercrime enables or facilitate different cybercrimes.

A. The Cascade Process

The TalkTalk case study roughly indicates six key stages at each of which cybercrime cascades downwards, though stages 3 to 5 can happen simultaneously. From this we can construct our cascade model.

Stage 1: Discovery and disclosure of vulnerability

A person (it might be a hacker or not) discovers a vulnerability on a company's software, website, or application. They have different options to take. A 'White Hat' (ethical) hacker might try to obtain a legitimate financial reward by informing the owning company of their vulnerability through bug-bounty programmes, such as those listed on BugCrowd[7] and HackerOne.[8] In such cases little more is heard about the vulnerability because it has been patched and the bug finder is paid off. When a disclosed vulnerability is ignored by the system owner, however, White Hat hackers may threaten to publicly disclose its existence to put pressure on the company to fix it. This was the case of 9to5mac discovering the Apple's FaceTime eavesdropping exploit [26].

When the motivation is driven by moral, revenge or reputation enhancement reasons, the offenders may post the information on web forums or, as did 'Fearful' alias 'Glubz', on TalkTalk's website [21]. In the TalkTalk breach, the flaw was also reported, allegedly by someone other than 'Fearful', via xssposed.org [21]. This is where information about the vulnerability can drift from ethical hacker (White hat) to the cracker (Black hat). Experienced malfeasants, for example, will seek to exploit vulnerabilities, especially if it is zero-day, by disclosing them to friends or by selling them on to anybody who will pay for the information.

The disclosure of a vulnerability, when shared, sold or made public, is a primary tipping point for the cascade effect, unleashing the first crime frenzy of offenders trying to exploit the vulnerability.

Stage 2: Exploitation of vulnerability

Once the information contained in the data is circulated (either privately or in public) and the vulnerability has not been fixed, there is nothing to stop offenders from exploiting it. Offenders may use a different range of tools to exploit the vulnerabilities, for example, to distract security personnel and possibly weaken a system with a DDoS attack. DDoS attacks open the door for tools to penetrate the victim's weakened system, for example, using an SQL injection to extract the data. In the case of TalkTalk, as mentioned earlier, it was reported that the vulnerability was exploited as many as 14,000 times [11]. Whilst this again raises the metaphor of a crime frenzy, it is highly likely many of those exploitations had little or no visible impact and suggests that many were exploiting the vulnerability for recreational purposes. Often, simply because they could, or out of intellectual curiosity, however, exploiting the vulnerability paves the way to another tipping point which unleashes further stages (3-5) of the cascade effect where the cybercrime and harm becomes a stark reality.

Stage 3: Monetization of vulnerability

Exploiting the vulnerability creates a power imbalance and leverage over the vulnerable (typically the system owner) which can then be monetized. The TalkTalk breach unveils one common path of monetization which is to demand the victim to pay a ransom for the stolen copies of the data to be returned. In other cases, such as ransomware, upon the payment the victim

[7] Bug Crowd <https://www.bugcrowd.com/bug-bounty-list/>

[8] Hackerone <https://hackerone.com/bug-bounty-programs>

is given a code which allegedly decrypts the data encoded by malware. In the TalkTalk case Hanley, Allsopp and Kelley demanded a ransom which, unless paid, would lead to them dumping the data in public. Alternatively, the data could be dumped into the black market or sold on, as in the case of 'Courvoisier' [40]. In another case it was revealed that a hacker called 'Martian' bragged that she or he could make £150,000 in profits by selling the data of 10,000 victims [49]. What this tells us is that information arising from the data dump can be monetized. This can be achieved by using the threat of the consequences of exposure to directly extort victims from whom the data was taken – the system owner or the data subject. It can also be done by selling on the data, especially if it is personal or if it contains confidential personal or business information, such as trade secrets. This data dump constitutes another key tipping point in explaining the cascade effect.

Stage 4: Buying or Trading Data (to commit further crimes)

Offenders (typically fraudsters) may purchase the data to defraud or otherwise victimise, especially financial data which allows frauds such as carding (trafficking fraud devices), card-not-present and account takeover to take place. Sometimes the financial data may not be strong enough to be used for, say, carding, but could enable an attacker to perform less sophisticated forms of attack. This was the case in the TalkTalk breach because 15,656 banking details and sort codes were stolen [18] and several victims reported being defrauded as a result of the TalkTalk breach. Unfortunately, it is currently not possible to actually ascertain how many had their banking details/sort code exploited as a direct result of the breach and how many fell victim to pretexting (scams based upon the hack, see further on). Yet, the number of victims is potentially 15,656 people. At the same time, much of the data may not have been so easily monetizable because it was not complete, which would lead to stages 5 and 6.

Stage 5: Turning Data into Crime or Retaining, Refining or Collecting Additional Data for Future Offending

At times, the data is not enough to enable offenders (fraudsters) to immediately victimize. This was the case with TalkTalk customers' personal information (156,959) which was not attached to the corresponding 15,656 banking details and sort codes. Yet, offenders may still want to acquire personal data as a source of intelligence to commit other cyber-assisted crimes or even more traditional forms of frauds. Potentially, this unleashes a further crime frenzy, targeting (in the TalkTalk case) as many as 156,959 customers.

Offenders may also delay using the data so that its capability to victimize can be enhanced by amalgamating further data from different sources about the victim. The attackers may, for example, develop spam lists for sending out phishing emails to acquire more personal data, which they may use to develop their databases of victims. Attackers may put up the repackaged information on sale, as in stage 3&4, which paves the way for another (mini) cybercrime tipping point. This was the case with 'Courvoisier's' actions, possibly also in relation to the TalkTalk breach as he appeared to promise more information than was revealed to have been breached by news reports and the ICO [18].

Stage 6 Pretexting: Exploiting confusion to commit new crimes

As discussed earlier, a separate group of offenders – scammers– not related or known to the original hackers or even the downsellers, may also try to exploit the data subjects' confusion in the wake of the publicity from a data breach. Known as pretexting, scammers socially engineer a response from victims by drawing on prevailing public concerns such as a disaster, cancer, or in this case a hack, to develop a plausible story or pretext to deceive their victims [1]. So, using the very public TalkTalk breach as a pretext, scammers pretended to be from the company, knowing that there was a reasonable chance of the user being either a TalkTalk customer or being simply worried about the news reports of hacks. Once they got the victim worried, the pretexters would talk them through resetting their passwords so that other attackers could not use their compromised information to victimize them, which, of course, was both an irony and a lie. In other reported cases, scammers used different pretexts often posing as employees of UK Internet service providers (e.g. BT or TalkTalk), saying that they had been authorized by Microsoft to provide technical support [12]. Gallagher, an Ars Technica journalist, was targeted by pretexting scammers in a different scam and wrote about his experience. "The scam (…) seeks to convince would-be victims to install remote-access software on their computers and then to set up recurring credit card billing for technical support or anti-virus software" [12].

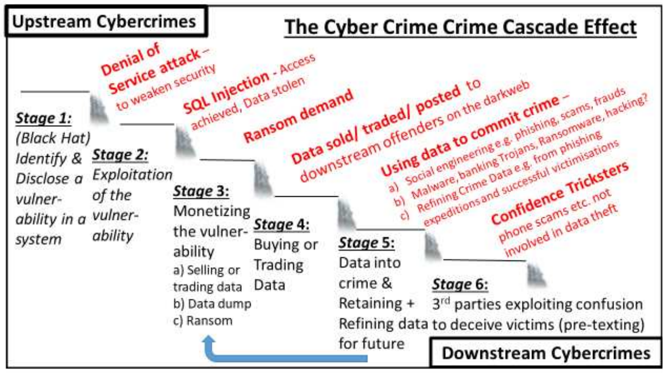
A further 'crime stream' underlying stages 3-6 are the monetizers who help to facilitate downstream crimes (and possibly some upstream). They launder money, extract or broker currency from crimes. Depending upon the scale of the crime, they may collect money or turn bitcoin and other cryptocurrencies from ransomware into fiat money or employ money mules to extract money in cash from live accounts via ATMs or transfer money in short-term legitimate accounts that they 'loan' or set up specifically for the purpose. We argue that the presence of monetizers introduces the potential for the development of organized criminal groups, but it is a potential observation which needs much further research to establish.

B. Reflections on the Cybercrime Cascade Effect

Figure 1 (below) illustrates the relationship between the first six stages. Steps 1-3 of the cascade are upstream crimes that roughly correspond to categories of cyber-dependent crime [46]. Steps 4-6 (and monetizers) are downstream crimes that largely correspond to cyber-enabled (facilitated by the internet) and cyber-assisted crimes (using the internet for convenience) [46]. As stated earlier, these 'stages' are ideal types and we expect to find variations of the them in practice, but they demonstrate the key tipping points where upstream crimes cascade further downstream. Furthermore, each tipping point at stages 1-6 involves different forms of interaction between offenders, such as chat forums, underground data markets, cybercrime-as-a-service or networks of money mules. These 'pinch points' are locations where law enforcement, crime prevention and regulatory resources can be directed to make for more effective action.

The hallmark of the cascade-effect-crime-flow downstream is that the resulting 'crime frenzy' that tends to occur is very hard for law enforcement to follow. What is more, upstream and downstream crimes tend to be committed by separate (groups of) offenders against different victim groups for very diverse motivations. All of which complicates and frustrates the basic process of conceptualization and ultimately reflects upon both the way that the media covers these offences and how they are viewed by law enforcement personnel, influencing the reporting, recording, investigative and prosecution processes.

Figure 1 The Cybercrime Cascade Effect


Upstream Cybercrimes
The Cyber Crime Crime Cascade Effect
Denial of Service attack – to weaken security
SQL Injection - Access achieved, Data stolen
Ransom demand
Data sold/ traded/ posted to downstream offenders on the darkweb
Using data to commit crime –
a) Social engineering e.g. phishing, scams, frauds
b) Malware, banking Trojans, Ransomware, hacking?
c) Refining Crime Data e.g. from phishing expeditions and successful victimisations
Confidence Tricksters phone scams etc. not involved in data theft
Stage 1: (Black Hat) Identify & Disclose a vulner-ability in a system
Stage 2: Exploitation of the vulner-ability
Stage 3: Monetizing the vulner-ability
a) Selling or trading data
b) Data dump
c) Ransom
Stage 4: Buying or Trading Data
Stage 5: Data into crime & Retaining + Refining data for future
Stage 6: 3rd parties exploiting confusion to deceive victims (pre-texting)
Downstream Cybercrimes

As a result of the cascade effect, cybercrimes therefore appear to be dis-organized in terms of their structure when viewed through the lens of centralizing[9] contemporary crime and organised crime narratives [22][44]. But, those narratives are often oversimplified and misapplied because the offending activities are actually distributed rather than centralised. Distributed, not only in terms of the ways that offenders organize themselves to work together to commit offences via, for example, chat forums where they obtain skills, information and also collaborators, but also to actually deliver the offending activity [44].

So, the organization of upstream cybercrime is distributed rather than centralized, as is often assumed. Furthermore, recent research [48] has identified different levels of sophistication in the distribution of criminal labour with regard to upstream and downstream cybercrimes. The upstream, big data-related cybercrimes are being committed by primary offender groups who range from Amateurs (e.g. wannabees and script kiddies), Hobbyists (e.g. ethical and unethical hackers) and Professionals (IT skills for hire) [8][48]. All of which are being enabled via cybercrime services operated by a secondary offender group – the cybercrime kingpins. These kingpins are a separate level of offenders who enable cybercrime to take place and whose services to are commissioned by both upstream and downstream primary offenders to help them commit their crimes [48].

It is important to note that each kingpin performs a different function but together form a facilitating infrastructure for the cybercrime ecosystem. Data brokers sell or trade data; Crimeware-as-a-service (CAAS) providers enable DDoS or ransomware attacks. Spammers use the data to send out mass email campaigns. Darkmarket operators run market places on the dark web that sell software, data and cybercrime services. Botherders run the networks of compromised computers to send out spams, or CAAS outputs. Crime IT service brokers write code or trade vulnerabilities. Monetizers run the operations that extracts fiat money out of various cybercrime operations, for example, via cryptocurrency and systems of employing money mules [48].

It is important to note here that the distinction between kingpin activities is not always so clear in practice. This is because of the necessary interdependency between their roles, but also the wherewithal for more than one function to be run by an individual or group depending upon the scale of the cybercrime operation involved. For example, on a small scale an individual or small group can perform the various functions themselves, but as the scale of the operation gets larger, then there is a necessary division of labour and specialisation of skills [48].

In fact, the business models of each of the brokerages are built around the different ambitions of customers. An analysis of a stresser operation, used to launch DDoS attacks, for example, found different levels of service ranging from a discounted entry level which provided 10 minutes of access to the stresser at a discounted cost (and even a $2 one off trial!), through to a premium VIP rate costing many thousands of dollars. The system was clearly being used by both upstream and downstream primary offenders and catered for each [28]. In the case of those involved in the TalkTalk attack, it is possible/likely that they will have used the cut down and trial rates available to them – though with considerable impact.

IV. CRIMINAL JUSTICE INTERVENTION

According to BAE Systems, who were engaged by TalkTalk to investigate the attack, there might have been up to 10 attackers in total [5], however the police arrested six individuals and all but one (a boy from London) were convicted. 'Courvoisier', who was mentioned earlier and was possibly involved in the sale of data, was also convicted.

The first arrest took place shortly after the breach and was of a 17-year-old who had discovered and exploited the vulnerability [59]. Unnamed, for legal reasons, he pleaded guilty to seven offences against the Computer Misuse Act 1990. In addition to the TalkTalk breach, he had also breached a small database of staff and students at the University of Manchester, the library at the University of Cambridge and a company supplying badges for martial arts. He was sentenced to a 12-months rehabilitation order [31] at a Norwich Youth Court, which, like all Magistrates Courts, does not record the court proceedings. It seems that the same person, now aged 19, is now being prosecuted and tried for stealing personal data and selling it on to criminals [63]. Bisson [5] reported that the Metropolitan Police also arrested a 15-year-old in Northern Ireland whose identity was protected, but who was named by some news sources which he sued (including Twitter) and subsequently

[9] E.G. always looking for a 'Mr Big' and assuming a higher form of organization that protects its criminals and seeks to increase its power.

settled confidentially [3]. It is not clear from reports how he exploited the TalkTalk vulnerability.

The third person arrested was Daniel Kelley from Llanelli, South Wales, who was 18 at the time of arrest. He exploited the vulnerability "to steal credit card information, and then sent a ransom message to TalkTalk demanding 465 bitcoins (worth $125,550 at the time, according to historical pricing data compiled by CoinDesk)". He threatened to dump the data if the ransom was not paid [10]. Kelley was found in possession of personal data and credit card information belonging to 5000 people which he had put on sale on a "hacker type site" [32]. The blackmail charge was eventually dropped because "the trial was not in the public interest", although he was due to be sentenced on February 25th and warned that he faced a jail sentence [50]. As of April 2019, the sentence was unknown.

The fourth and fifth were friends Matthew Hanley [4] and Connor Allsopp, 20 and 18 respectively at the time they were arrested, from Staffordshire [5]. According to news reports, Hanley exploited the TalkTalk vulnerability and supplied Allsopp with breached personal information of 8000 TalkTalk customers, so that Allsopp could monetize the data. Hanley recommended Allsopp not to sell the data for less than £1000 [37]. Both Hanley and Allsopp also supplied data for hacking to a third party known as "Reign" [11] and "revealed details of how they broke into the site to other people to then exploit" [59]. They were both handed custodial sentences in 2018. Note that some news reports depict Kelley, Hanley and Connor as members of a 'gang' [56].

Finally, Grant West, aka 'Courvoisier' [40], allegedly linked to selling the TalkTalk data, among data from many other breaches, was arrested and tried, though news reports do not mention the TalkTalk breach.

Apparently 'Martian', the alias used by a person selling the data online, was not caught on this occasion, nor was 'Reign', who received part of the data from Allsopp. Interestingly, the only TalkTalk-related posts that can be retrieved from historical data scraped from the now-defunct AlphaBay forum relate to Martian.[10] Courvoisier's posts are no longer available.

A. Reflections on the TalkTalk case

This analysis of the TalkTalk breach shows how complicated and distributed, apparently disorganized, a data breach is. There is clearly a disconnect between the very high media profile of the case, the police investigation and the subsequent prosecution(s). Moreover, notwithstanding the fact that the case was very high profile, the news reports do not enable a clear picture to be established of the relationship between the individuals involved. Or, for that matter, what happened to those who were arrested (e.g. the London-based boy) or those subsequently identified as fraudsters (e.g. Courvoisier and Martian). Furthermore, it is also very difficult to connect the claim that there were 14,000 attacks with the scant number of arrests.

Even the safer path of obtaining court materials is frustrated by the fact that Court's records are not easily accessible, if at all; Magistrate Courts do not transcribe the hearings and most Crown Court cases are unreported. At the time of writing, we are still waiting for authorization to receive transcripts for the sentencing of Hanley, Allsopp and Kelley.

V. Reactions by TalkTalk and Breach Prevention

On October 26th TalkTalk reported a sequential attack, but the online community corrected them, stating that they were the victims of an SQL injections [5]. On November 6th TalkTalk revealed that the actual scope of the breach against its website was "much more limited than initially suspected". As reported by the BBC, the company stated that the personal information of 156,959 customers was compromised and that 15,656 sets of banking details and sort codes were stolen [5]. Additionally, 28,000 payment cards were "obscured" and "cannot be used for financial transactions". On November 11th TalkTalk estimated the damage of the breach to range between £30 million and £35 million resulting from the "loss of online sales and service capability" [5]; TalkTalk recently increased it to £77m [59].

TalkTalk's former CEO eventually admitted that they got their cybersecurity wrong [59]. Indeed, according to the Information Commissioner's Office, TalkTalk was not aware of the existence of the unpatched webpages that were exposed to SQL injections, which Symantec refers to as 'rudimentary forms of attack' [30]. They had failed to implement even the most basic security measures, for example, user input was not validated at source and the vulnerable webpages used outdated software libraries [18] (p. 4). It is interesting that SQL injection was the method by which the initial offenders attacked the TalkTalk webpages in July 2015 and on 2&3rd September that year [18] (p. 9); both well before the main data breaches in October 2015.[11] With the benefit of hindsight, had Talktalk implemented basic security and data protection measures after the initial breaches, they would arguably have not been attacked in October 2015 and not faced the ensuing public storm.

VI. Big Data Crime and the Law

The synergy between the implementation of data protection rules and cybercrime prevention has long been discussed, but mostly remained in data protection circles [33][20][34] rather than cybersecurity practice. Yet, following the entry into force of the GDPR, it is becoming clearer that the early adoption of technical and organisational measures to protect personal data would reduce the occurrence of breaches [30][34]. Not only does the UK National Cyber Security policy [15] acknowledge the preventative role of the GDPR [52], but also it leaves all the preventative 'heavy lifting' to data protection rules. Indeed, the GDPR and related Data Protection Act 2018 [54] provide for a suite of measures to curb cybercrimes. Firstly, an entity that does not take adequate measures to safeguard personal data faces harsh administrative fines (Art. 83) which can reach £17 million or up to 4 per cent of the entity's total worldwide annual turnover [34]. What is more, Article 82 of the GDPR gives victims who have suffered from material or non-material damage as the result of an infringement of the GDPR, such as a

[10] We are very grateful to Dr Adam Hardy for advice on this point.

[11] An interesting timeline of the intervention by the Information Commissioner's Office is available at https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded/

data breach, the right to claim compensation (though with caveats). Theoretically, the claim for damages could ironically extend to the offenders who have abused victims' personal data, because, by virtue of being in possession of stolen personal data, the offenders could be construed as data controllers in their own right and subject to the terms of the GDPR, including its sanctions.

Secondly, the English and Wales Court of Appeal already recognized a claim for non-pecuniary damages in Google Inc. v Vidal-Hall & Others [53]. The same Court also recognized that misuse of private information can be construed as a tort (specifically for the purposes of gaining permission to service proceedings outside of the UK).

Thirdly, under s.170 of the DPA 2018 it is an offence for a person knowingly or recklessly to obtain or disclose personal data without the consent of the controller, as well as to procure the disclosure of personal data to another person without the consent of the controller. Furthermore, it is an offence for a person to sell, or to offer to sell, personal data obtained in such circumstances. This includes the offer to sell personal data, such as an advertisement indicating that personal data is or may be for sale. Unfortunately, offences under s.170 DPA 2018 are no longer punishable with a custodial sentence, because the DPA 2018 repealed s.77 and s.78 of the Criminal Justice and Immigration Act, which allowed a maximum custodial sentence of two years. Actually, s.77 and s.78 were never relied upon, because the necessary secondary legislation implementing such powers "was never introduced, despite repeated lobbying by the ICO" [61]. Things may change, however, because in November 2018 the ICO brought a prosecution for the first time under the Computer Misuse Act 1990 which was guided by the principles established in R v Rollins [2010] UKSC 39 [62] and which resulted in a custodial sentence [60].

Tortious and, especially, criminal liability leading to custodial sentences may have more of a significant effect on deterrence than penalties. This point was repeatedly recommended by the ICO and other interested parties who submitted evidence to the parliamentary inquiry following the data breach [14]. We anticipate that the findings of our cascade effect research will present a strong argument for encouraging the use of all instruments and related penalties across the regulatory spectrum against unauthorized data exfiltration [34][35]. Furthermore, findings of upcoming research may inform regulatory changes [65][48]. For instance, the importance of protecting the confidentiality of data other than personal data does not find equivalence in criminal law in the UK, as the primary objective of the Computer Misuse Act is to safeguard the integrity of computers [51] (p. 72). Furthermore, s.2 of the Computer Misuse Act1990 [55], read together with s.17, may not lay down strong enough rules to counter the effect of data dumps and onward sale.

VII. Conclusion and Way forward

Our analysis of the TalkTalk case study suggests that tipping points occur at each stage of the cascade model, for example the disclosure of a vulnerability, its exploitation, followed by its monetization (selling data), then other offender groups buying it, then using it directly to commit crimes or refine it to commit future crime, and finally third parties using the pretext of the original attack to deceive victims. The TalkTalk case study not only illustrates the cascade of cybercrimes from upstream to downstream crimes but it also enables us to make five observations in conclusion.

Our first observation is that the analysis and discussion illustrates the complexities of online crime groups, especially their diverse and distributed (even disorganized) nature when compared with contemporary organised crime narratives [22][44]. Moreover, the case study details workings that appear quite different in a number of ways from more traditional crime groups. In TalkTalk, not only had they not met in the flesh, but only Hanley and Alsop seemed to know each other in person (possibly also Kelley). Moreover, the groups appear to have been aware of each other and in competition with one another. This is because the ability to monetise a data breach displays elements of rivalrous resources, in that consumption by one group reduces the ability of another group to consume it. The groups mainly conversed on chat forums [37][4] and Skype.

Our second observation is the relative youth of the offenders caught when compared with the seriousness of the impact of their offending, although it is very possible that others who exploited the breach were not caught. Also significant is that their profiles indicate that they are not the burly street criminals that the criminal justice is designed for [46].

Our third observation is that the motivations of those caught may have led them to become, for want of a better description, 'low hanging fruit' and may have made themselves more easily identifiable to law enforcement. This is because they were not primarily motivated by financial gain. As more than one said in court, the underlying motivation was intellectual curiosity and to impress friends in order to increase their status in the reputational hierarchy of their group (crime forum). It is almost as if they were acting in a computer gaming, rather than serious crime frame of mind. To this end, the TalkTalk vulnerability was simply a vehicle. This certainly applies to one of the two minor offenders convicted who did not seem to exploit the information for financial gain. The person sentenced at Norwich Magistrate's Court may have initially not been motivated by financial gain, but he is now reportedly being prosecuted for stealing and selling personal data [63], so a 'drift' in to delinquency may be taking place. The extent to which this reflection applies to the three young adults convicted remains to be seen and we hope will be clarified by the court proceedings when they are obtained. All three displayed financial acumen, shown not only by asking for a ransom but also pricing the data in accordance to their value. Moreover, in his judgment the judge did stress their ability to comprehend the seriousness of the impact of their offending. Ongoing research under the CRITiCal project is seeking to unveil the relationship between age at time of offending and motivation. Future planned court observations will increase our understanding of the prosecution process when establishing the precise nature of criminal intent, but also punishment.

Our fourth observation is that the case sends some blunt messages to business organisations to keep on top of their computer security during a time where new attack vectors appear to be matching or even exceeding attempts to keep systems technically secure [27]. Former TalkTalk CEO Harding attributed the hack to legacy technology which she described as “the IT equivalent of an old shed in a field that was covered in brambles” [59]. This observation places even more emphasis upon the human factors involved to make the right decisions in terms of computer security policy and data protection. It also highlights the need to regulate in a consistent manner the prevention and minimization of data breaches and security incidents [34] and equip the criminal justice system with adequate deterrence.

Our fifth and final observation relates to how hard it is to find out information about events in order to research them. There is no single reliable data source of information, there is no database for arrests, prosecutions and outcomes. But it also becomes evident that there are historical, legal, bureaucratic and professional reasons why this is the case. In one way it demonstrates the ‘myth of data’ that seems to exist.

This early conceptualization of the cybercrime cascade effect is drawn from a small part of a much larger interdisciplinary project (CRITiCal) which explores changes in the cybercrime landscape resulting from cloud technologies and IoT, of which Big Data Crime is one such development [47][35]. These findings will provide a framework for exploring and analysing cloud crimes and identifying a broader pool of offender types to help tailor appropriate interventions against them to prevent further transgression and prevent cybercrime. The findings of this detailed study inform our larger investigation based on mixed methods and a blend of legal empirical analysis and criminological analysis. This will include the analysis of additional case studies of data breaches and cybercrimes displaying ‘cascade’ elements and the related sentencing of responsible individuals, analysis also based on data science and machine learning. It will eventually help corroborate the relative importance of tipping points, such as the publication of details of a vulnerability and the dump of data, as well as make recommendations for changes to the legal framework and its implementation within the criminal justice system.

Acknowledgment

We would like to thank our project partners at Newcastle and Durham Universities and the various policing and judicial agencies which have helped us in conducting this research. We also thank colleagues from the Centre for Criminal Justice Studies at Leeds. Needless to say, the views expressed in this paper are our own views and not those of either partners funding agency or other participants in the project.

References

[1] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Hoboken, NJ., Wiley, 2008.

[2] BBC (2015, Oct. 25) TalkTalk: Customer believes firm hacked 'months ago,' BBC News Online. [Online]. Available: https://www.bbc.co.uk/news/av/uk-34631315/talktalk-customer-believes-firm-hacked-months-ago

[3] BBC (2016, Jan. 19) TalkTalk hack attack: Northern Ireland boy who was arrested settles claim against Twitter, BBC News Online. [Online]. Available: http://www.bbc.co.uk/news/uk-northern-ireland-35445935

[4] BBC (2018, Nov. 19) TalkTalk hack attack: Friends jailed for cyber-crimes, BBC News Online. [Online]. Available: https://www.bbc.co.uk/news/uk-england-stoke-staffordshire-46264327

[5] D. Bisson. (2015, Nov. 25) The TalkTalk Breach: Timeline of a Hack, (UPDATED 11/25/15). Tripwire. [Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-talktalk-breach-timeline-of-a-hack/

[6] R. Broadhurst, P. Grabosky, M. Alazab, & S. Chon. (2014) “Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime,” International Journal of Cyber Criminology, vol. 8, no. 1, pp. 1-20.

[7] Channel 4 (2016, Jan. 22) TalkTalk hack: a closer look at the scammers, Channel 4 News. [Online]. Available: https://www.youtube.com/watch?v=mYvVtsqNk6Q

[8] R. Chiesa, S. Ducci, & S. Ciappi. (2006) H.P.P. The Hacker Profiling Project: A General Overview, paper to the hack.lu 2006 conference. 19- 21 Oct., Luxembourg.

[9] G. Corfield. (2017, Jun. 28) Four Brits cuffed in multimillion-quid Windows tech support call scam probe. Malicious chats mostly came from India, say police, The Register. [Online]. Available: https://www.theregister.co.uk/2017/06/28/4_brits_arrested_windows_tech_support_scam/

[10] J. Cox. (2017, Feb. 21) Convicted TalkTalk Blackmailer Warns Young Hackers About Falling Into Crime, Motherboard. [Online]. Available: https://motherboard.vice.com/en_us/article/pgxa3m/convicted-talktalk-blackmailer-warns-young-hackers-about-falling-into-crime

[11] K. French. (2017, Apr. 26) Computer geeks face jail after admitting £42million hack attack on telecoms giant TalkTalk's website, MailOnline. [Online]. Available: https://www.dailymail.co.uk/news/article-4448834/Computer-geeks-admit-42million-hack-attack-TalkTalk.html

[12] S. Gallagher. (2017, Jun. 28) London police arrest four in Windows support scam bust, Ars Technica. [Online]. Available: https://arstechnica.com/tech-policy/2017/06/london-police-arrest-four-in-windows-support-scam-bust/

[13] S. Greenhill. (2015, Nov. 4) Beware the scammers who claim to be from TalkTalk: Listen to the call that reveals fraudsters' dirty tricks, This is Money. [Online]. Available: https://www.thisismoney.co.uk/money/bills/article-3302475/Beware-scammers-claim-TalkTalk-Listen-call-reveals-fraudsters-dirty-tricks.html

[14] HOC (2016, Jun. 20) Cyber Security: Protection of Personal Data Online, First Report of Session 2016–17, HC 148. House of Commons, Culture, Media and Sport Committee. [Online]. Available: https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/148.pdf

[15] HM Government (2017) National Cyber Security Strategy 2016 to 2021, Cabinet Office, revised 11 September [Online]. Available:

https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[16] A. Hutchings and T. Holt. (2015) “A Crime Script Analysis of the Online Stolen Data Market,” British Journal of Criminology, vol. 55, pp. 596-614.

[17] E. Hutchins, M. Cloppert and R. Amin. (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Lockheed Martin. [Online]. Available: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[18] ICO (2016, Sep. 30) Monetary Penalty Notice against TalkTalk Telecom Group PLC. Information Commissioner’s Office. [Online].

[19] IOCTA (2018) Internet Organised Crime Threat Assessment 2018. EUROPOL. [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

[20] B-J. Koops and R. Leenes. (2014) “Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law,” International Review of Law, Computers & Technology, vol. 28, no. 2, pp. 159-171.

[21] M. Krebs. (2015, Oct. 25) TalkTalk Hackers Demanded £80K in Bitcoin, Krebs on Security. [Online]. Available: https://krebsonsecurity.com/2015/10/talktalk-hackers-demanded-80k-in-bitcoin/

[22] A. Lavorgna and A. Sergi. (2016) “Serious, Therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom,” International Journal of Cyber Criminology, vol. 10, pp.1-23.

[23] R. Leukfeldt and J. Jansen. (2015) “Cyber Criminal Networks and Money Mules: an analysis of low-tech and high-tech fraud attacks in the Netherlands,” International Journal of Cyber Criminology, vol. 9, no. 2, pp. 173-184.

[24] R. Leukfeldt, A. Lavorgna and E. Kleemans. (2017) “Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime,” European Journal on Criminal Policy and Research, pp. 287-300.

[25] A. Martin. (2015, Nov. 13) TalkTalk hired BAE Systems' infosec bods before THAT hack, The Register. [Online]. Available: https://www.theregister.co.uk/2015/11/13/talktalks_security_revealed/

[26] B. Mayo. (2019, Jan. 28) Major iPhone FaceTime bug lets you hear the audio of the person you are calling … before they pick up, 9to5mac. [Online]. Available: [Online]. Available: https://9to5mac.com/2019/01/28/facetime-bug-hear-audio/

[27] T. Morbin. (2018, Jun. 4) InfoSec 2018. TalkTalk hack - lessons learned - the board perspective, SC Media. [Online]. Available: https://www.scmagazineuk.com/infosec-2018-talktalk-hack-lessons-learned-board-perspective/article/1466618

[28] R. Musotto, D. Wall. (2018) Are Booter Services (Stressers) indicative of a new form of organised crime group online?, UNODC Linking Organized Crime and Cybercrime Conference, School of Global Studies, Hallym University, Chucheon, South Korea, 7-8 June.

[29] J. Oltsik. (2014, Oct. 8) Proofpoint report exposes details about cybercrime division of labour and malware architecture, CSOnline [Online]. Available: https://www.csoonline.com/article/2693226/cisco-subnet/proofpoint-report-exposes-details-about-cybercrime-division-of-labor-and-malware-architecture.html

[30] Z. Précsényi, G. Nanni, R. Arandjelovic and R. Gallego (2019) Security and Breach Notification under the GDPR: the Symantec recommended operational approach, Symantec (Unpublished).

[31] C. Page. (2016, Dec. 13) TalkTalk hack: 17-year-old sentenced to 12-month rehabilitation order. Teen also has his iPhone and hard drive confiscated, The Inquirer. [Online]. Available: http://www.theinquirer.net/inquirer/news/2479524/talktalk-hack-17-year-old-sentenced-to-12-month-rehabilitation-order

[32] E. Pennink. (2016, Dec. 13) Teenage TalkTalk hacker Daniel Kelley warned he faces jail, The Independent. [Online]. Available: https://www.independent.co.uk/news/uk/crime/talk-talk-hacker-daniel-kelley-warned-he-faces-jail-a7472671.html

[33] M-G. Porcedda. (2012) Data Protection and the Prevention of Cybercrime - The EU as an Area of Security? EUI Working Papers LAW No. 2012/25.

[34] M-G. Porcedda. (2018) “Patching the patchwork: appraising the EU regulatory framework on cyber security breaches,” Computer Law and Security Review, vol. 34, no. 5, pp. 1077-98.

[35] M-G. Porcedda and D. Wall. (2018) “Data crime, data science and the law,” in V. Mak, E. Tjong Tjin Tai & A. Berlee (eds) Research Handbook on Data Science & Law. London: Edward Elgar.

[36] Press Association (2018a, 25 May) Hacker jailed for selling Asda and Uber customers' data on dark web, The Guardian. [Online]. Available: https://www.theguardian.com/technology/2018/may/25/hacker-jailed-for-selling-asda-and-uber-customers-data-on-dark-web

[37] Press Association (2018b, Nov. 19) Two men jailed for involvement in TalkTalk hacking, The Guardian. [Online]. Available: https://www.theguardian.com/uk-news/2018/nov/19/two-men-jailed-talktalk-hacking-customer-data

[38] Proofpoint (2014) Analysis of a cybercrime infrastructure, Proofpoint. [Online]. Available: https://cdn2.vox-cdn.com/uploads/chorus_asset/file/2340876/proofpoint-analysis-cybercrime-infrastructure-20141007.0.pdf

[39] Sky (2017, Aug. 10) TalkTalk fined again after customer data breach by Indian firm Wipro, Sky News. [Online]. Available: https://news.sky.com/story/talktalk-fined-again-after-customer-data-breach-by-indian-firm-wipro-10982359

[40] R. Spillett. (2018, May 25) Hacker dubbed 'Courvoisier' who stole 78 million usernames and passwords to sell on

the dark web with cyber attacks on Uber, Argos and Asda is jailed for more than 10 years, MailOnline. [Online]. Available: https://www.dailymail.co.uk/news/article-5770819/Hacker-dubbed-Courvoisier-jailed-10-years.html

[41] Symantec (2019) Internet Threat Security Report 2019, Symantec.

[42] S. Tonkin. (2015, Nov. 1) TalkTalk customers' bank details stolen in massive online hack are already up for sale at £1.62 a time, MailOnline. [Online]. Available: https://www.dailymail.co.uk/news/article-3298943/TalkTalk-customers-bank-details-stolen-massive-online-hack-sale-1-62-time.html

[43] R. Wainwright and F. Cilluffo. (2017, Mar.) Responding to cybercrime at a scale: operation Avalanche – a case study, Issue Brief # 2017 -03, EUROPOL. [Online]. Available: https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf

[44] D. Wall. (2015) "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime", The European Review of Organised Crime, vol. 2, no. 2, pp. 71-90.

[45] D. Wall, (2015, Oct. 28) The TalkTalk hack story shows UK cybersecurity in disarray, The Conversation. [Online]. Available: https://theconversation.com/the-talktalk-hack-story-shows-uk-cybersecurity-in-disarray-49909

[46] D. Wall. (2017) "Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing", in R. Brownsword, E. Scotford and K. Yeung (eds) The Oxford Handbook of the Law and Regulation of Technology, Oxford: Oxford University Press, pp. 1075-1096.

[47] D. Wall. (2018, Jan.) "How Big Data Feeds Big Crime," Current History: A journal of contemporary world affairs, pp. 29-34.

[48] D. S. Wall. (Forthcoming) Cybercrime KingPins'

[49] S. Wright and C. Cortbus. (2015, Oct. 31) Hacked TalkTalk information on sale to organised fraud gangs for £1.60 a time, Mirror. [Online]. Available: https://www.mirror.co.uk/news/uk-news/hacked-talktalk-information-sale-organised-6744695

[50] BBC (2019, Jan. 28) TalkTalk hacker Daniel Kelley's blackmail charge dropped, BBC News Online. [Online]. Available: https://www.bbc.co.uk/news/uk-wales-47025847

[51] J. Clough (2015), Principles of Cybercrime, Cambridge: Cambridge University Press.

[52] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

[53] Google Inc v Vidal-Hall & Ors [2015] EWCA Civ 311 (27 March 2015), http://www.bailii.org/ew/cases/EWCA/Civ/2015/311.html

[54] Data Protection Act 2018, https://www.gov.uk/government/collections/data-protection-act-2018

[55] Computer Misuse Act 1990, https://www.legislation.gov.uk/ukpga/1990/18/contents

[56] H. Martin, (2019, Jan. 28), Computer hacker, 21, faces jail for stealing customer details from TalkTalk in massive data breach which cost the mobile network £77m, Mailonline. [Online]. Available: https://www.dailymail.co.uk/news/article-6641315/Computer-hacker-faces-jail-stealing-customer-details-TalkTalk.html

[57] ICO (2017) Monetary Penalty Notice against TalkTalk Telecom Group PLC. Information Commissioner's Office. [Online]. Available: https://ico.org.uk/media/action-weve-taken/mpns/2014626/mpn-talktalk-20170807.pdf

[58] G. White, (2017, March), Inside the TalkTalk 'Indian scam call centre', BBC NewsOnline. [Online]. Available: https://www.dailymail.co.uk/news/article-6641315/Computer-hacker-faces-jail-stealing-customer-details-TalkTalk.html

[59] R. Chirgwin, (2018, Nov. 20), TalkTalk hackhack duoduo thrownthrown in the coolercooler: 'Talented' pair sentenced for ransacking ISP. The Register. [Online]. Available: https://www.theregister.co.uk/2018/11/20/talktalk_pair_jailed/

[60] ICO (2018), Six month prison sentence for motor industry employee in first ICO Computer Misuse Act prosecution, The Information Commissioner's Office. [Online]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/six-month-prison-sentence-for-motor-industry-employee-in-first-ico-computer-misuse-act-prosecution/

[61] Out-law.com (2018), ICO prosecutes under Computer Misuse Act, Ou-tlaw.com. [Online]. Available: https://www.out-law.com/en/articles/2018/november/ico-prosecutes-computer-misuse-act-/.

[62] ICO. The Information Commissioner's Response to the Leveson Report on the Culture, Practices and Ethics of the Press, The Information Commissioner's Office. [online]. Available: https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2154/ico_response_to_leveson_report_012013.pdf

[62] EdwinCoe LLP (2018), ICO sends data thief to prison, Blog - 19/11/2018, EdwinCoe LLP. [Online]. Available: https://www.edwincoe.com/blogs/main/ico-sends-data-thief-to-prison/

[63] C. Cunningham. (2019) 'Norwich teen who hacked TalkTalk on trial for stealing people's personal data and selling it to criminals', Eastern Daily Press, 2 April, https://www.edp24.co.uk/news/crime/norwich-talktalk-hacker-back-in-court-1-5971048

[64] D Collier. (2011) Understanding Process Tracing, Political Science and Politics 44 (4)

[65] M.G. Porcedda (forthcoming), 'Prosecuting Data Crime: The courts, data crime and the cascade effect'