BILETA Response to Review of the Computer Misuse Act 1990

Prepared on behalf of the British Irish Law, Education and Technology Association (BILETA) by Dr Kim Barker, Dr Lisa Collingwood, Dr James Griffin, and Dr Felipe Romero–Moreno

The British and Irish Law Education Technology Association (BILETA) was formed in April 1986 to promote, develop and communicate high-quality research and knowledge on technology law and policy to organisations, governments, professionals, students and the public. BILETA also promotes the use of and research into technology at all stages of education. The present inquiry raises technological, economic and legal challenges that our membership explores in their research. As such, we believe that our contribution will add to the public discourse and the inquiry on the future of CMA 1990.

Domain name and IP address takedown and seizure

Q1. What should be the threshold for the use of this power, what tests would an application have to meet and what safeguards should apply to it?

Pursuant to human rights caselaw, the development of any new power to allow law enforcement agencies to take control of domains and IP addresses against alleged criminal activity should always be subject to State authority's oversight and ensure that the affected parties and/or individuals have access to appropriate safeguards and an effective remedy before the courts.[1]

Although so far, at the international level there is no consistent caselaw concerning the conditions to find primary or secondary liability of DNS providers, following seminal England and Wales High Court caselaw,[2] it would be arguably possible in the UK to grant injunctive relief against DNS providers, under Section 37(1) of the Senior Courts Act 1981. To do so, there is a specific threshold and relevant safeguards, which should be applied and satisfied.

To begin with, in terms of the threshold for using the suggested power: firstly, DNS providers should be considered internet intermediaries under the third sentence of the Enforcement Directive (which is retained EU Intellectual Property law as per section 6(7) of the EU Withdrawal Act 2018); secondly, operators and/or users of these DNS providers should also be infringing the DNS services (e.g. supporting criminality such as fraud and computer misuse); thirdly, operators and/or users of such DNS providers should also be using the DNS services to infringe;
and lastly these DNS providers should also have knowledge of this (i.e., being previously notified of the alleged criminality).[3]

---

[1] See *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [318]; *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [110] and [122]; *Klass and others v Germany* App no 5029/71 (1979–1980) 2 EHRR 214 [55]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [59], [122]; *Amann v Switzerland* App no 27798/95 (2000) 30 EHRR 843 [60]; See also Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [123]; C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] [17].

[2] Section 37(1) of the Senior Courts Act 1981 provides that 'The High Court may by order (whether interlocutory or final) grant an injunction … in all cases in which it appears to be just and convenient to do so.' See *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014) [74].

[3] *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014) [139].

In this context, it is worth noting that CJEU caselaw suggests that it is disproportionate to request law-abiding internet intermediaries to monitor all information for infringing content without a notice, which narrows down the monitoring obligations to specific content.[4] This is also confirmed by domestic trade mark caselaw from European countries such as, Germany, France, Belgium, Sweden and Austria, which stresses that DNS providers are not compelled to monitor information and domains for infringing content prior to court orders or a rightholder's notification.[5] Therefore, intermediary liability might just be contemplated if the DNS provider fails to stop offering its service to the unlawful site following an infringing notice.[6]

Moreover, regarding relevant safeguards, pursuant to seminal England and Wales High Court caselaw, there are also some principles, which should be applied and satisfied: (i) the injunction must be necessary to protect the rights and freedoms of others; (ii) the injunction must also be effective i.e. requiring DNS providers to prevent unlawful access to alleged criminality or at least making it difficult to attain;[7] (iii) the injunction must also be dissuasive against users;[8] (iv) the injunction must not be excessively costly or complicated i.e. considering the difficulty and cost of complying with the order;[9] (v) the injunction must also avoid barriers to legitimate trade e.g. the measures taken must be specifically targeted thus users being able to access the DNS providers to lawfully access information;[10] (vi) the injunction must also be fair and equitable and strike a 'fair' balance between the right to property, the right to freedom expression, the right to privacy, the right to protection of personal data, the freedom to conduct a business, and the right to a fair trial and an effective remedy; and (vii) the injunction must also be proportionate[11] i.e. assessing whether alternative measures may be less restrictive.[12]

Q2. Which organisations should have access to the power?

It should be noted that, for instance, as injunctions in England and Wales, interdicts in Scotland are commonly granted as a preventative remedy by the court to stop a wrong, which is anticipated or being committed, or is infringing a party's rights. Thus, provided that the development of any new power is being subject to State authority's supervision and ensures that the parties and/or individuals affected can rely on an effective remedy before the courts, arguably there are a number of law enforcement agencies, which may have access to that power. For example, while in the UK, law enforcement agencies such as, the National Crime Agency, the Metropolitan Police or the City of London Police might be able to rely on this power, the latter could also be available in response to a request from other overseas law

[4] C-70/10 *Scarlet Extended SA Société Belge des Auteurs, Compositeurs et Editeurs Scrl (SABAM)* [2011] ECR I-11959 [47].
[5] German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 30 – Störerhaftung des Registrars; German Federal Supreme Court (BGH) of 17 May 2001, I ZR 251/99 – ambiente.de; District Court Stockholm of 19 May 2015, B 6463-13 and Svea Court of Appeal of 12 May 2016. B 5280-15; Commercial Court Brussels of 9 August 2013, 2012/12072/A; Court of Appeal Versailles of 15 September 2011, 09/07860 – Association AFNIC vs SAS Francelot; Court of Appeal Paris of 19.10.2012 – Air France et als v. AFNIC/EuroDNS; Austrian Federal Supreme Court (OGH) of 12.9.2001, 4 Ob 176/01p – fpo.at II.
[6] https://www.wipo.int/export/sites/www/enforcement/en/pdf/working-paper-dns-study.pdf
[7] C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and anor* [2014] All ER (D) 302 (Mar) [62].
[8] *Ibid* [171].
[9] C-70/10 *Scarlet Extended SA Société Belge des Auteurs, Compositeurs et Editeurs Scrl (SABAM)* [2011] ECR I-11959 [48]; C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA v Netlog NV* [2012] 2 CMLR 18 [46]; C-324/09 *L'Oréal SA and others v eBay International AG and others* [2012] All ER (EC) 501 [139].
[10] C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and anor* [2014] All ER (D) 302 (Mar) [56]; C-324/09 *L'Oréal SA and others v eBay International AG and others* [2012] All ER (EC) 501 [140].
[11] *Golden Eye (International) Ltd v Telefónica UK Ltd* [2012] EWHC 723 (Ch), [2012] RPC 28 [116]; C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271 [61]-[68]; C-70/10 *Scarlet Extended SA Société Belge des Auteurs, Compositeurs et Editeurs Scrl (SABAM)* [2011] ECR I-11959 [42]-[46]; C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA v Netlog NV* [2012] 2 CMLR 18 [42]-[46], [50]-[53]; C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and anor* [2014] All ER (D) 302 (Mar) [46].
[12] *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014) [158].

enforcement agencies including the US Federal Bureau of Investigation, the Drug Enforcement Administration, the International Criminal Police Organization, or the Europol.

In this regard, it is worth mentioning that there is a tendency in Europe to rely on self-regulatory approaches accompanied by state oversight concerning DNS blocks by Internet Service Providers (ISPs).[13] These self-regulatory schemes have been reached by ISPs and rightholders in several Member States such as, Germany,[14] Denmark[15], and the Netherlands.[16] There are two approaches. On the one hand, the Dutch and Danish scheme compels a court injunction against one domestic ISP in a sample case, that is subsequently followed without requiring any other court injunction by the rest of domestic ISPs belonging to that scheme.[17] On the other, the German approach entails an initial examination by a self-regulatory organization (including former judges from the Federal Supreme Court) and a further check by the German Federal Network Agency, which oversees telecommunications and ensures net-neutrality.[18]

Moreover, there are several countries, which rely on no-fault injunctions such as, Australia, Singapore, and India. For instance, under the Australian regime, the addressee of a no-fault blocking injunction is considered a 'carriage service provider'[19] as per section 78 of the Telecommunications Act 1997. However, this does not seem to cover a DNS operator. Conversely, in Singapore, the definition of internet intermediary includes 'a person who provides services relating to or provides connections for the transmission or routing of data',[20] which would appear to cover DNS providers. Additionally, in the copyright context, in India, the High Court of New Delhi has ordered injunctive relief against ISPs to block access to infringing sites, finding ISPs the key solution to solving the online piracy problem.[21]

Q3. What will a statutory power enabling the seizure of domain name and IP addresses allow that voluntary arrangements do not currently allow?

As previously noted, in Scotland interdicts are like injunctions in England and Wales, which are granted as a preventative remedy by the court to stop a wrong that is anticipated or being committed or is violating a party's rights. Unlike the current voluntary arrangements, a new statutory power enabling the seizure of domain name and IP addresses for law enforcement agencies, would allow injunctive relief against registrars and registries, thus both still being subject to injunctions to disable/suspend the domain names. This would be particularly the case even if they were not a defendant or party in legal proceedings.

For example, serving as a case study, although in the context of IP infringement, in the United States, registrars and registries can also be subject to injunctions without proving fault on their

[13] Nordemann, Website Blocking under EU Copyright Law, p. 374 et seqq., in Rosati, Routledge Handbook EU Copyright Law, 2021.
[14] www.cuii.info
[15] https://sharewithcare.dk/
[16] https://www.acm.nl/en/publications/agreement-among-internet-providers-and-copyright-holders-regarding-blocking-websites-illegal-content
[17] See for the Dutch system: https://www.acm.nl/en/publications/agreement-among-internet-providers-and-copyright-holders-regarding-blocking-websites-illegal-content
[18] See for the German system: www.cuii.info
[19] Section 115A, Copyright Act 1968.
[20] Section 193A, as inserted by section 47, Copyright (Amendment) Act 2004
[21] UTV Software Communication Ltd vs 1337X.To and Ors (2019) paragraph 72. Judgment and opinion available at: https://indiankanoon.org/doc/47479491/.

part. Importantly, the issuance of these types of injunctions is based on Federal Rule of Civil Procedure 65(d)[22] regarding the scope and contents of restraining orders and injunctions.[23]

It is worth pointing out that the US ruling in *the North Face Apparel Corp v Fujian Sharing Imp & Exp Ltd Co*, (which is a seminal decision regarding registries and registrars), having the Court found that the defendant websites were involved in counterfeiting and trademark infringement, it also held that even if the infringing registry was not a party or defendant in litigation, injunctive relief against registrars and registries was not only allowed but also appropriate, under Federal Rule of Civil Procedure 65(d)136.[24] Thus, as the WIPO notes, US federal courts have consistently used Federal Rule of Civil Procedure 65(d) to order a wide range of non-party intermediaries such as, domain name registries and registrars, search engines, hosting providers, and reverse proxies to stop providing their services to sites infringing IP rights. While these internet intermediaries have taken the view that they are simply 'passive' providers and thus not in 'active concert or participation' with the unlawful sites, the courts have found otherwise, ordering injunctions to require such non-party intermediaries to stop providing services to the unlawful sites.[25]

That said, however, as flagged above, pursuant to human rights caselaw, this statutory power should always be subject to State authority's oversight (e.g., the courts or the relevant data protection authorities), ensure that individuals and/or parties affected have access to an effective remedy before the courts to assess the legitimacy of any action taken, as well as putting in place appropriate safeguards to prevent abuse.[26] In this regard, it should be noted that while the UK still remains subject to the Human Rights Act 1998, which gives effect to the European Convention on Human Rights 1950 in UK law, retained EU caselaw, which applies EU Charter rights would still seem to bind the UK courts.

Q4. What activity would we ask the recipients of an order to undertake that they do not undertake under voluntary arrangements?

In terms of potential activities that the recipients of domain name orders should undertake, it would be advisable for the government to follow the Internet Corporation for Assigned Names and Numbers' Guidance for Domain Name Orders. According to the ICANN, as domain name registration providers such as, registrars or registries need specific information to allow them to comply with court injunctions or investigate regulatory or legal actions there is information,

---

[22] Federal Rule of Civil Procedure 65(d) provides: '(1) Contents. Every order granting an injunction and every restraining order must:
(A) state the reasons why it issued; (B) state its terms specifically; and (C) describe in reasonable detail – and not by referring to the complaint or other document – the act or acts restrained or required. (2) Persons Bound. The order binds only the following who receive actual notice of it by personal service or otherwise: (A) the parties; (B) the parties' officers, agents, servants, employees, and attorneys; and (C) other persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B).'

[23] https://www.wipo.int/export/sites/www/enforcement/en/pdf/working-paper-dns-study.pdf

[24] *The North Face Apparel Corp. v. Fujian Sharing Imp. & Exp. Ltd. Co., No. 10* CIV. 1630 (AKH), 2011 WL 12908845 (S.D.N.Y. June 24, 2011).

[25] See e.g., *Artista Records, LLC v. Tkach*, 122 F. Supp 3d 32 (S.D.N.Y. 2015); *Showtime Networks, Inc. v. Doe 1*, Temporary Restraining Order and Order to Show Cause, No. 15-CV-3147 (CD Cal. April 30, 2015); *Warner Bros. Ent., Inc., v. Doe*, Preliminary Injunction Order, No. 14-CV-3492 (SDNY May 29, 2014); *AACS-LA v. Shen*, Order, No. 14-CV-1112 (SDNY Mar. 4, 2014); see also https://www.wipo.int/export/sites/www/enforcement/en/pdf/working-paper-dns-study.pdf

[26] See *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [318]; *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [110] and [122]; *Klass and others v Germany* App no 5029/71 (1979–1980) 2 EHRR 214 [55]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [59], [122]; *Amann v Switzerland* App no 27798/95 (2000) 30 EHRR 843 [60]; See also Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [123]; C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] [17].

which should always be submitted along with those orders or actions bearing in mind the following questions: (1) who is making the request? – the complainant (plaintiff), or the respondent (defendant), or it is court of record; (2) who are the key points of contact? – issuers of requests are advised to supply some form of official verifiable contact information (e.g. name, email, postal address, phone number), and state if any contact information supplied remains confidential; (3) what type of request is? - the request should clearly state if it is a court order (attached), or regulatory action, or third party request for action accompanied by valid evidence confirming the third party request; (4) what is the expected response time? - time and date by which the actions stated in the court or regulatory action must be carried out; (5) is there an intention to get records concerning the domain at the same time the domain is seized? – the court or regulatory action should detail and define all types of documentation or records sought including the span of time; (6) how is the domain name registration record to be modified? – it is necessary to state all the modifications requested or ordered; (7) how is domain name status to be modified? - prevent transfer of domain name, or prevent updates to domain name registration, or delete domain name; (8) is the domain name to be transferred to a different sponsoring registrar? – assign domain to new registrar detailed; (9) is the party, which provides name resolution service (DNS) to be modified? - modify authority for DNS, or modify DNS configuration of the domain; (10) is name resolution service (DNS) to be suspended? - suspend name resolution (DNS) i.e., 'seize and take down'; (11) is redirection to a text of notification page needed? - redirect domain name to text of notification page i.e., 'seize and post notice'; (12) is redirection of Internet hosting needed? - redirect to host operator i.e., 'seize and operate'; an (13) what should WHOIS for the domain name show? - WHOIS information display modification or disclose proxy/private registration.[27]

Q5. How can voluntary agreements, which are the preferred route for take downs, be protected?

When it comes to protecting voluntary agreements concerning take downs, it would also be advisable for the government to: (i) avoid any narrow interpretation of website content abuse; and (2) rely on 'trusted notifier' or 'trusted flagger' arrangements.

Firstly, it is worth noting that while ICANN requires registrars and registries to maintain arrangements to tackle abuse of domain names, these arrangements do not provide an exhaustive definition of what 'abuse' is.[28] However, in 2019, a coalition of registrars and registries produced the DNS Abuse Framework[29] recognizing four types of 'Website Content Abuse'. These include: (1) child sexual abuse content; (2) unlawful online circulation of opioids; (3) human trafficking; and (4) credible and explicit incitements to violence.[30] Notwithstanding, following the terms of the DNS Abuse Framework, these four types of content abuse do not entitle a registrar or registry to suspend/disable the website domain name without a court order.

Secondly, in terms of safeguarding voluntary agreements regarding take downs, it is also possible to adopt trusted notifier/flagger arrangements. Practically speaking, through these agreements, the notifier/flagger must first contact the domain registrar and the internet hosting provider to seek redress (i.e., preventing the hosting provider to host the website, thereby taking it offline, and suspending its domain name by the registrar). If the notifier/flagger gets either no response or an unfavourable one from the registrar and the internet hosting provider,

[27] https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf
[28] https://www.wipo.int/export/sites/www/enforcement/en/pdf/working-paper-dns-study.pdf
[29] https://dnsabuseframework.org/
[30] https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

then the registry must examine the notifier/flagger's written notification and decide if suspension of the domain name is appropriate.[31]

Q6. Should seizure mean the legal control and ownership (at least of the lease period) of domain names and IP addresses, or more temporary action such as sinkholing, pass to the law enforcement agency responsible for the order? Would law enforcement agencies pay for the lease?

Any seizure process should be to strict established protocol. There are two main risks:

a) That the current procedure is used to get around sufficient judicial oversight of web blocking orders as currently used under s.97A CDPA 1988 for copyright works.

b) That the mutual legal aid agreements with third countries be used, again, to avoid judicial oversight.

The consultation document makes a lot of use of the word 'criminal.' Whilst there are of course numerous criminal acts of the sort referred to in the consultation document, there are many edge cases which have proved controversial in the past. Most notable in this regard are actions for alleged copyright infringement, where existing safeguards against overuse have been established. Unfortunately, there is precedent that the proposed criminal provisions could be used against websites wholesale, before an adequate hearing is held in court with clear arguments from all parties concerned. This could prove detrimental to well-known services such as archive.org, where a legitimate service could be swiftly and entirely blocked due to allegations of copyright infringement either from within the UK or a third country. This could endanger many legitimate services, and cause substantial serious harm to access legitimate content on the Internet. It is worth noting that the proposal in the consultation document does not clearly protect such legitimate services, as the document does not indicate how such a service would be able to provide a defence to allegations of alleged criminal behaviour / illegality. This is a significant and serious potential overreach of the proposed legislation.

That being said, there is clearly a benefit in certain cases of illegality e.g. illegal substances, weapons, child pornography at one extreme, to prima facie pirate streaming sites on the other, where seizure of this sort could enable the posting of clear messages about the illegality of the site – as occurred in Operation 404. Furthermore, as noted in the consultation itself, data obtained through seizure could be used to identify victims of fraud and close down existing botnets. Trusted third parties may wish to be involved, e.g. to assist with security breaches in their own software, but this involvement should be strictly regulated to prevent future data breaches.

Once granted, law enforcement agencies or trusted third parties (under strict regulation) should pay for the lease, though account needs to be taken of which enforcement agency is being used regarding availability of finances. It might be sensible to arrange a central fund. Another reason for such a fund is to ensure that it is possible to compensate any right holders for loss caused by the granted of an order, particularly given the mutual legal assistance provisions with third countries.

Finally, it is suggested that extreme caution should be employed in the tone of proposed legislation. The reliance on criminality disguises the reach of the law over those borderline

[31] https://www.wipo.int/export/sites/www/enforcement/en/pdf/working-paper-dns-study.pdf

cases such as those concerning copyright works. There is a difference between a case of the sales of illegal weapons on the black market and, say, a website hosting a remix of a film that might potentially fall within fair dealing provisions. This distinction is not adequately made in the consultation document, yet extension of scope could become a defining application of the legislation.

Q7. If action is taken by law enforcement, should that be done for both the domain name and the IP address, and are there different recipients for orders for these?

Domain name and IP addresses. The reason for this is orders will in effect be pointless otherwise. However, there needs to be sufficient oversight for the granting of orders over both, e.g. due to the difficult position that those administering the registers might be in, for example, conflicting responsibilities between regulating bodies and State laws, or between a Registry, Registrant and Registrar. The latter group will be aware that orders obtained without sufficient oversight could endanger legitimate businesses, in breach of existing contractual agreements, rights and responsibilities. To this end, therefore, it is critical that any procedure should have clear judicial guidance and oversight, as detailed elsewhere in our answers.

Q8. Should multiple domains / IP addresses feature on one application or will separate applications be required?

Due to the proliferation of mirror sites for closed websites, it is clearly necessary that these should be caught by any blocking order and thus one application alone should be sufficient for variants. Currently, the system used under s.97A CDPA 1988 is, beyond the pleasing of shareholders, essentially useless in terms of practical application. However, beyond variants for mirror sites, there should be separate applications required to ensure sufficient judicial oversight.

Q9. Should there be scope for an emergency interim order to be made in advance of a hearing for a full order?

This question is vague as to its intent. It would imply that an emergency interim order is different to the usual interim order. If the former, then this should be avoided at all costs. The risk of damage to legitimate companies is substantial in the event of an interim order being granted. The balancing of interests could mean the loss of companies or jobs at legitimate companies, versus a temporary loss of a typically larger company seeking an enforcement action. Whilst an undertaking of damages could be taken by the enforcement agency, this may not be sufficient and it is possible the enforcement agency may not be able to cover final costs, or be out of jurisdiction for all practical purposes.

However, history has shown that interim orders can still be well reasoned decisions. There is no reason not to have a standard interim order, but this order does need to be sufficiently reasoned, with a judge being made to ensure that the procedure is not being used to undermine the public interest in being able to access legitimate internet sources.

Q10. Should there be an opportunity for extensions to the order?

If this is an interim order, the order should be only for the length required for inquiry. The possibility of abuse is again too great, with damage occurring to legitimate businesses. We have seen in the past the damage caused with the initial uses of search orders for fishing expeditions. This abuse of process should not be tolerated again, as it could substantially

undermine – for example - the delicate balance of copyright law. Furthermore, it should be kept in mind that future technological developments in fields such as quantum computing are likely to substantially enhance the existing interests and legal protections of right holders, which is another reason to caution against another extension of existing legal rights.

Power to Preserve Data

Q1. Which agencies should be able to use this power?

The power – should it exist – should be limited so as to ensure that bodies are not overreaching in seeking to ensure data preservation. At a maximum, the power should extend to law enforcement agencies such as the National Crime Agency, the Serious Fraud Office, and police forces.

Other bodies should not have wide ranging powers to preserve data. This is a particularly important balance to strike given the tensions around privacy rights and data access, and the potential for it to exacerbate pre-existing power imbalances, especially for marginalised and / or vulnerable groups.

Q2. Are there any problems associated with preserving data that we need to consider?

The power must be limited to ensure that bodies do not overreach. Irrespective of the limit – or otherwise – the power, there must be regulatory oversight of those seeking to exercise the power, recording and reporting of the instances where such a power has been exercised, and the offences related to it.

The potential for additional costs to be incurred by those required to preserve data is another significant consideration, especially were such a proposed power to be an open-ended one. Added to this are concerns surrounding interoperability of data, and the accessibility of data.

The ease – or otherwise – of preserving data, especially digital data and ensuring it is in a readable form, especially if it is to be preserved for a prolonged period of time. Similarly, issues of volume of data may also arise. High-profile instances of archiving digital data running into storage issues given the volume of data concerned is likely to be a challenge, subject to the parameters of such a preservation order. For instance, the US Congress has changed its approach to archiving tweets, from every public tweet initially, to now operating on a selective basis because of the volume of tweets that would have to be collated.[32] This is not the only example – other instances of digital archiving of important emails at newspapers exist as alternative approaches.[33] Both examples serve as indicators of the problem of scale when it comes to preserving data.

As an associated issue, if the volume of data for which preservation is sought is vast, questions persist about which data will or should be selected, if any. Further unknowns surround the how of making any such selection. Similar questions exist about the interplay between the proposed power to preserve, and the right to have information deleted. What are the criteria for such selections? And more importantly, who decides? Is there a framework for the making of such decisions?

---

[32] US Library of Congress, 'Update on the Twitter Archive at the Library of Congress' (December 2017) https://blogs.loc.gov/loc/files/2017/12/2017dec_twitter_white-paper.pdf.

[33] Chris Baraniuk, 'The online data that's being deleted' BBC Future (15 July 2021) https://www.bbc.com/future/article/20210715-the-online-data-thats-being-deleted.

The Open Data Charter[34] principles:

1. Open by Default
2. Timely and Comprehensive
3. Accessible and Usable
4. Comparable and Interoperable
5. For Improved Governance and Citizen Engagement
6. For Inclusive Development and Innovation.

should be remembered in deciding the breadth of the power and the agencies to which it shall be given.[35]

Q3. Should there be a time limit on the preservation order? If so, what should that be?

The Budapest Convention time limit on this is more than reasonable and any proposed power should not extend beyond 90 days.[36]

In any event, it would be particularly useful for there to be consistency across regimes in terms of an upper limit of time for any such preservation order.

Q4. Who should be responsible for covering any costs of preservation? How should they be determined?

The costs should be borne by the agency seeking to exercise the power. A reasonable fee per day / month up to a maximum should be set which is claimable by the party incurring the expense of the preservation in order to comply. This could operate on a scheme similar to the claims[37] that are available to those completing a period of jury service.

Q5. Are the existing powers in the Police and Criminal Evidence Act 1984 Schedule 1 already sufficient to allow preservation?

Yes. The special procedure should be followed and equally applicable here. Given the exercise of powers under PACE, there is little to be gained in adding additional powers which are potentially supplementary or contradictory to PACE.

If law enforcement bodies are to be the bodies given such a power, they should already be familiar with PACE so there is best practice in ensuring that this remains the default for powers relating to the preservation of data – data is a form of evidence and therefore falls within the PACE powers. It is particularly important that there is consistency here given the judicial oversight which is attached to PACE.

Data copying

Q1. What is the gap in current legislation, and what effect does that have?

There is a gap in the current legislation as the CMA covers unauthorised **access** to computer data and the unauthorised taking or **copying of data** is not covered by the Theft Act. The effect is that certain types of behaviours are not being captured by current legislation, but should be.

[34] https://opendatacharter.net/.
[35] It is to be noted that the UK Government as a G8 member introduced an Open Data Charter Action Plan in 2013 https://www.gov.uk/government/publications/g8-open-data-charter-national-action-plan.
[36] Convention on Cybercrime, Article 16 (2001) https://rm.coe.int/1680081561.
[37] https://www.gov.uk/jury-service/what-you-can-claim-if-youre-an-employee.

It is therefore certainly arguable that there should be a new offence under the CMA of *possession/copying of illegally obtained data*

Under the CMA, the copying of data would attract the penalties listed under section 1 (unauthorised access to computer material carries a maximum penalty of up to 12 months in prison on a summary conviction, or two years on indictment, or a fine or both). This could be considered an insufficient penalty to deal with the seriousness of the criminality. It is noted that some stakeholders suggest that this does not deter criminals and may not represent a sufficient disincentive given the financial gains that may be possible from the commission of the activity and that a new offence such as this should attract a higher penalty (see 3. below).

However, there is a further consideration. Whilst it is positive that specific legislation has been created for the specific offences under the CMA, the range of offences is growing and the legislation may not adequately tackle the myriad of new offences that the advancing technology may spawn. It may be a mistake to continually amend legislation that has a different remit just so that new, previously unimagined offences can be captured by existing legislation[38].

Q2. Are there examples of where harm is caused by the absence of an offence?

If a person e.g. holds the data but did not commit the CMA offence, but the objective in holding the data is the subsequent **commissioning** of an offence – e.g. copying the data in order to gain a pecuniary advantage / in order to perpetrate fraud subsequently.

Q3. What is the appropriate penalty if such an offence was created?

To convict and sentence a person, a court must be satisfied that the offence is made out and legal sanctions must be tailored to reflect the severity of a situation[39].

Changes to legislation have tended to lead to an array of prosecutions concerning a seemingly disparate range of behaviours and any changes in the scope of the CMA will inevitably raise questions related to consistency.

Therefore, given that applicable guidelines exist in relation to, e.g. fraud and money-laundering, the same would need to be available in respect of revisions to offences under the CMA so as to ensure a consistent approach.

Ultimately, the objective would be for the penalty for the new offence under the CMA of *possession/copying of illegally obtained data* to be at least consistent with the Theft Act. For example, fraud carries a maximum sentence of up to **five years** imprisonment.

---

[38] L Collingwood, "Electronic communications media : how to regulate the hate!" *Information and Communications Technology Law* Volume 31 (3), 2022, 382-399 https://www.tandfonline.com/doi/epdf/10.1080/13600834.2022.2088065?needAccess=true&role=button, last accessed 14 March 2023

[39] L Collingwood, "Electronic communications media : how to regulate the hate!" *Information and Communications Technology Law* Volume 31 (3), 2022, 382-399, 391 https://www.tandfonline.com/doi/epdf/10.1080/13600834.2022.2088065?needAccess=true&role=button, last accessed 14 March 2023

As detailed above, it is debateable whether the best approach is for existing legislation to be revised or for new legislation to be developed. As the CMA was never intended to apply to *possession/copying of illegally obtained data,* prosecuting the wider offence under it is a controversial step.

When current legislation fails to address the fast-moving online environment, this may require the introduction of new, proportionate and more effective criminal offences and legislation as opposed to a mere adaptation of existing legislation, when instead there is a need to develop legislation[40].

[40] L Collingwood, "Electronic communications media : how to regulate the hate!" *Information and Communications Technology Law* Volume 31 (3), 2022, 382-399, 399 https://www.tandfonline.com/doi/epdf/10.1080/13600834.2022.2088065?needAccess=true&role=button, last accessed 14 March 2023