Police Practice and Research
An International Journal

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/gppr20

Perception or reality? Data protection legislation as an impediment to law enforcement information sharing, and ways to prevent it

Rebecca Phythian & Stuart Kirby

To cite this article: Rebecca Phythian & Stuart Kirby (21 Feb 2025): Perception or reality? Data protection legislation as an impediment to law enforcement information sharing, and ways to prevent it, Police Practice and Research, DOI: 10.1080/15614263.2025.2465262

To link to this article: https://doi.org/10.1080/15614263.2025.2465262

Published online: 21 Feb 2025.

POLICE PRACTICE AND RESEARCH
https://doi.org/10.1080/15614263.2025.2465262

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS Check for updates

Perception or reality? Data protection legislation as an impediment to law enforcement information sharing, and ways to prevent it

Rebecca Phythian [a] and Stuart Kirby [b]

[a]Edge Hill University; [b]University of Central Lancashire

ABSTRACT

Information sharing is integral to tackling organised crime and terrorism. Academic studies and government inquiries both highlight the failings of law enforcement agencies in this endeavour, regularly citing data protection legislation as an impediment. To explore this issue a thematic analysis of UK law enforcement practitioner interviews ($n = 41$) together with a quantitative analysis of UK law enforcement data breaches (n = 28,654) was conducted. Results show practitioners identify legislation as a blockage to information sharing, however this is based on a lack of understanding, rather than the failings of the legislation itself. It was also discovered that data breaches generally occur through individual mistakes rather than malicious intent and are not punitively sanctioned by regulators. It suggests leaders at both law enforcement and government level could streamline policy and reduce bureaucracy through simplifying and co-ordinating the implementation processes involved.

ARTICLE HISTORY
Received 6 November 2024
Accepted 5 February 2025

KEYWORDS
Information sharing; legislation; data protection; data breach; law enforcement

Introduction

Sharing information between and across organisations is a crucial process for law enforcement agencies across the world (Abrahamson & Goodman-Delahunty, 2014; College of Policing [CoP], 2020). Whilst intrinsically linked to the general safety and well-being of citizens, its importance has magnified due to the increased international nature of organised crime and terrorism (Rusi, 2023). Considerable evidence shows law enforcement agencies often fail to share information effectively or efficiently (Peters, 2023), illustrated by high profile incidents such as the UK Soham murders (Bichard, 2004), the U.S.A. 9/11 attacks (Farivar, 2021), and the Pickton case in Canada (Dhillon & Bailey, 2014). As failures in information sharing are often associated with fatal consequences, this is a crucial area to improve.

Legislation has a critical role in regulating information. Only 15% of countries, found within parts of Africa, Asia and South America, have no legal framework to protect data and privacy (United Nations Conference on Trade and Development [UNCTAD], 2025). Whilst impracticable to list all legislation here most frameworks share similar principles – whether it be China's Personal Information Protection Law 2021, the Australian Privacy Act 1988, or the GDPR legislative framework that binds European Union (EU) countries. Specifically, nations attempt to find a balance between allowing information sharing to tackle crime, whilst simultaneously protecting legitimate privacy and human rights. However, the legalities

CONTACT Rebecca Phythian PhythiaR@edgehill.ac.uk Edge Hill University

surrounding information sharing is becoming increasingly complex, evidenced by studies from the UK (Bourton et al., 2022), Australia (Chaudhury & Choe, 2023), United States (Boyne, 2018), China (Zhang, 2024) and India (Greenleaf, 2023). Indeed, 'perceptions about legislation' is cited as one of the main barriers to multi-agency information sharing (Department for Education, 2023, p. 8).

As technological advances and the exponential rise of data in the 21st Century are expected to bring more legislative changes, understanding and resolving any friction associated with legislation becomes essential. This UK based study seeks to provide more detail in terms of how legislation is viewed and implemented in an operational environment. The literature review will show how legislation can be perceived, and how it continues to evolve. It will then provide law enforcement practitioner insight, to illustrate how professionals interpret and engage with the legislation. Finally, these views will be compared with what occurs in practice, specifically by examining recorded data breaches and their outcomes.

Literature review

In an increasing information led world, governments across all continents have introduced legislation to allow the legitimate sharing of information whilst ensuring human rights are protected. As an examination across all these nations is impracticable, this literature review will use the UK as an example, as its approach follows similar principles to other developed countries. It will commence with an overview of legislation relating to law enforcement information sharing. It will then explore how this legislation is implemented, together with an account as to what transpires when legal breaches occur.

In the UK, 2018 was labelled 'the year of data protection' (Mouzakiti, 2020, p. 363). As with other countries, comprehensive changes were introduced to address the challenges posed by 'the internet and digital technologies, social media and big data' (Information Commissioner's Office [ICO], 2019, p. 4). The Data Protection Act (DPA) 2018 was established to complement the General Data Protection Regulation (GDPR), apply the EU Law Enforcement Directive[1] (LED), and extend data protection laws following the UK's departure from the EU (ICO, 2019). The Act affects information processing 'to people, bodies or organisations … for any of the law enforcement purposes' (i.e., safeguarding, prevention, investigation) (ICO, 2019, p. 38). A few years later, during 2021, the UK GDPR was introduced to update the existing GDPR. It declared that when data processing is conducted for law enforcement purposes, by a competent authority[2] (e.g., police, courts, and prisons), the criteria under the DPA 2018 is satisfied. If not, data processing must comply with the wider UK GDPR rules (ICO, 2022a).

UK legislation allows non-law enforcement agencies to share information with a law enforcement agency if it is 'necessary and proportionate' (ICO, n.d.-a). Law enforcement agencies can also proactively share personal information with third parties under common law powers, provided there is 'a pressing social need' (e.g., a safeguarding concern) (CoP, 2020, National Police Chiefs' Council [NPCC], 2017). This is known as Common Law Police Disclosures[3] (CLPD), and its implementation is determined locally by chief officers (CoP, 2020). In the UK, law enforcement agencies are subject to other laws that affect information sharing. These include the Crime and Disorder Act 1998, and the Crime and Disorder Regulations 2009, which also provide the ability to share information for lawful reasons (CoP, 2020; Home Office, 2010). Within the legislation, UK law enforcement agencies are bound by either a *statutory obligation*, where disclosure of information is required (e.g., under the Police Act 1997, the Safeguarding Vulnerable Groups Act 2006, or in response to a court order), or a *statutory power*, where they possess the legal authority to share information with third parties but are not obligated to do so (CoP, 2020).

Challenges emerge when practitioners attempt to put the legislation into practice, as implementation failure is a common occurrence in Criminal Justice (Kirby, 2013). In essence, studies highlight a disconnect between executives who develop policy, the agencies who apply and enforce the policy, and those who implement it at street level (Carter et al., 2014; Williams, 1982). This can be compounded by convoluted language and legal terminology, which can differ across context, agency, and jurisdiction. Ultimately, this can generate confusion, especially for frontline staff who must interpret the legislation whilst also navigating many operational demands (Bennett Moses, 2020; Chan et al., 2022; Phythian & Kirby, 2022). These implementation issues can be further complicated when information sharing needs to take place with those partners who exist outside law enforcement, as it is governed by different legislation and specific directives (Chan et al., 2022; UK Parliament, 2023). Moreover, when information is stored in shared data warehousing platforms, 'determining *which* agency-specific legislation is relevant is itself potentially complex' (Chan et al., 2022, p. 9). These challenges are further exacerbated when international agencies are involved (see Birdi et al., 2021; Heusala & Koistinen, 2018). This complexity (Bourton et al., 2022) brings uncertainty about what information can be shared, with whom and under what circumstances (Chan et al., 2022; Peel & Rowley, 2010; Plecas et al., 2011).

Most organisations insist upon an audit trail to evidence the legitimacy of their actions. One aspect of this is the agreement to share information with a third party. In the UK formal templates are often used, such as a memorandum of understanding (MoU), service-level agreement (SLA) or information sharing agreement (ISA) (CoP, 2020). These formal agreements are often insisted upon, even if they are not mandatory, for example, when the information is shared under a statutory power. In practice, ISAs can be generated at a national level to facilitate the transfer of information from a national police system to an external agency. Similarly, local ISAs are commissioned in-force (i.e., by a police force lead) to enable information sharing at the local level. Force-to-force information sharing can be achieved through 'a formal request process or by providing direct access to force systems' (CoP, 2020) and does not necessitate a local ISA.

All agencies within their individual country will also have an accountability structure to monitor legislative compliance. In the UK, the ICO is responsible for ensuring the protection of information rights. A personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data' (ICO, 2022a). When they occur, law enforcement agencies are obligated to notify the ICO within 72 hours if there is 'a risk to the rights and freedoms of individuals' (ICO, 2022a). Non-compliance with Part 3 of the DPA 2018 can result in monetary penalties from the ICO (ICO, 2022a). However, to 'reduce the impact of fines', and promote 'better engagement' with the public sector, the ICO prefers to use 'warnings, reprimands and enforcement notices, with fines only used in the most serious cases', as well as 'publicising lessons learned and sharing good practice' (Blanchard, 2023; ICO, 2022b).

As such, UK police forces have tended to not face enforcement notices, although reprimands have been issued for various reasons, including human error and inappropriate disclosures (i.e., contextual information about a witness), process failures (i.e., uploading data to the UK Police National Database [PND]), and technology issues (i.e., unlawfully collecting personal data) (ICO, n.d.-a). In cases where individual officers have unlawfully accessed and shared data for personal rather than policing purposes, more punitive action has been taken (e.g., individual added to the national police barring list, fined, dismissed) (Hetherington, 2022; Karran, 2021). Reviews by the ICO have highlighted a lack of training and guidance, as well as inadequate risk assessments, policies and processes. It appears the most important criteria in deciding the outcome is understanding whether the matter is an organisational and/or individual data breach and whether malicious intent or human error was involved.

In summary, the legislative framework allows for the appropriate and lawful sharing of personal information (Department for Education, 2024) and the underpinning policies and procedures can

play a crucial role in mitigating perceived risks associated with sharing information (Abrahamson & Goodman-Delahunty, 2014). In fact, Akbulut-Bailey (2011, p. 56) argues absence of formal requirements can generate a perception that the task is 'discretionary', which could reduce information sharing or increase the risk of it being mishandled (Akbulut et al., 2009). However, this framework can also be complex. Chan and Bennett Moses (2017) highlight instances where formal protocol or legislation are used by officers as a rationale for withholding information, whilst there can be a reluctance of practitioners to exchange information due to a fear of breaching data protection laws (Monaghan et al., 2024; Shorrock et al., 2023; Waring et al., 2022). It should also be recognised that other issues, apart from the legislation, hinder information sharing. Sidebotham et al. (2016, p. 164) argue 'deep cultural barriers to effective information sharing between professionals' play a significant role.

Improving information sharing is a global concern, documented in the U.S.A. (i.e., Akbulut-Bailey, 2011), Canada (i.e., Plecas et al., 2011) and Australia (i.e., Chan et al., 2022). Previous suggestions to improve this include simplifying, clarifying and aligning legislation and guidance more effectively, as well as implementing short-term protocols and training (Centre of Excellence for Information Sharing, 2017; MacAlister, 2022; Peel & Rowley, 2010). Moreover, Treiber et al. (2022) discuss the use of applied cryptography techniques in privacy-enhancing technology to overcome many privacy concerns. Others endorse the increased use of IT (Nooteboom, 2003), as practitioners feel information sharing systems automatically comply with data protection requirements and provide accountability features, such as audit trails (Chan, 2003; Chan et al., 2022; Plecas et al., 2011). Unfortunately, the problems persist and as society becomes increasingly data-driven and interconnected, it is crucial to understand and address all matters that impede information sharing. As such, more detailed analysis is required, based on clear evidence to recognise the operational implications legislation has on information sharing by law enforcement practitioners.

Methods

This study adopts a mixed methods approach, which can be understood as, 'collecting, analyzing, and mixing both quantitative and qualitative data in a single study or series of studies' (Creswell & Plano Clark, 2007, p. 5). The synergy of both approaches can offer insight not available through the separate strands (Fetters & Freshwater, 2015), thereby providing, 'breadth, depth of understanding and corroboration' (Johnson et al., 2007, p. 120). As such, the use of mixed methods serves as a distinct methodological approach (Todak & Somers, 2024). In this study the data was obtained using a sequential design, initially starting with semi-structured interviews, to establish how law enforcement professionals consider legislation impacts upon information sharing. Second, as it became apparent that legislation was viewed as a barrier to information sharing, the study examined actual data breaches facilitated using the UK Freedom of Information (FOI) Act 2000.

Stage 1: interviews

The purpose of the interviews was to establish whether legislation was seen by practitioners as an impediment to sharing information, and if so, why. Interviews were conducted with experienced intelligence professionals in the field of organised crime and terrorism, between April 2022 and April 2024 ($n = 41$). As law enforcement can be a difficult environment to penetrate from a research perspective (Skinns, 2023), support for the study was obtained from the National Police Chiefs' Council (NPCC). As trust and availability was also an issue, participants were recruited via professional networks, using purposive (i.e., participants were selected intentionally based on having relevant experience) and snowball (i.e., participants were asked to recommend other practitioners who had experience in this area) sampling techniques. All were invited to take part in either an online (Microsoft Teams) or in-person semi-structured interview. Eight questions were asked exploring the experience of

the individual, how policing and information management had changed, as well as good practice and barriers to improvement. The sample consisted of individuals from various organisations, including serving police officers, ex-police officers and police staff ($n = 28$; e.g., Merseyside Police, Greater Manchester Police, Gwent Police, Regional Organised Crime Units, the International Crime Coordination Centre, NPCC, National Crime Agency and Europol). It also included other government law enforcement agencies ($n = 6$; Border Force, FACT, HMRC and National Trading Standards), Non-Government Organisations (NGOs) and the commercial sector ($n = 7$; international technology company, local city councils and animal welfare groups). Roles ranged from Associate Director and Chief Constable to intelligence officer and analyst. All had significant experience in information sharing and could be expected to provide a more informed response than less experienced neighbourhood officers.

Interviews were audio recorded and transcribed verbatim, before undergoing thematic analysis in NVivo (Braun & Clarke, 2006, 2021), using both inductive (i.e., data driven) and deductive (i.e., theory driven) approaches. This involved generating initial codes semantically, with the codes then collated into themes and the themes undergoing review and refinement. The researchers did this independently and then collaboratively, to compare coding and discuss disagreements until a consensus was reached.

Stage 2: freedom of information requests

There are strengths and weaknesses of using FOI data (Monaghan et al., 2024). In this context it was felt beneficial as reporting a data breach is a legal requirement in the UK, therefore procedure was more likely to be consistent. Further, it provided a direct means to harvest data from across the UK, specifically to illustrate whether the legislation was being breached. FOI requests were submitted to 45 UK police forces, as well as British Transport Police, Civil Nuclear Constabulary, Ministry of Defence and the NPCC. The FOI request sought information on recorded incidents of data breaches from 2018 (the year the DPA was introduced) to 2022 (see Figure A1 in the Appendix) regarding the frequency, circumstances, and outcomes of such breaches.

Whilst numerous messages of clarification between the researchers and agencies took place, overall 32 agencies provided information on recorded incidents of data breaches. The most common reason for not providing data was Section 12 of the FOI Act (2000) (cost exceeding the appropriate limit) ($n = 14$), with agencies also referencing an inability to supply datasets due to information being held on multiple databases ($n = 9$). There were variations in the format and content of the data provided. For example, six agencies provided the number of breaches only (broken down by month and/or year), 15 agencies included information about the type of breach (either the category and/or a summary of the incident) and 23 agencies provided information relating to the ICO (i.e., the number of ICO referrals and/or the outcome). Furthermore, six agencies included 'near misses' or 'no breach' incidents,[4] and varying years of data were provided (e.g., five years of data provided by 23 agencies, three years by four agencies) with instances in which data for a complete year was missing (see Table A1 in the Appendix for an overview of the information provided by agency and Figure A2 for a summary of the entire process).

To facilitate the analysis, the data was collated into a single Excel spreadsheet for review. Due to variations in the datasets, the 'type of breach' variable was recategorised to allow comparison (see Table A2 in the Appendix for the coding dictionary). This process involved reviewing the existing categories presented in the data and applying the revised 'type of breach' categories to either i.) existing categories, or ii.) qualitative content (i.e., the summary, if categories were not provided). Quantitative data was then transferred to SPSS to undergo descriptive (i.e., average, percentages) and inferential analyses. Due to the non-normal distribution of the data (Shapiro-Wilk tests: $p < 0.05$), Kendall's tau correlations examined the relationships between the size of the force and (i) the number of breaches and (ii) the number of ICO referrals.

Results

This section initially presents the thematic analysis of the interviews, followed by the data breach findings.

Stage 1: interviews

All participants highlighted the importance of information sharing in tracking the movement of offenders and providing the evidence to connect them with crime. In terms of how legislation facilitated or hindered this process the analysis discovered five themes, which are described below.

i) Limited understanding: Participants discussed a lack of understanding of data protection legislation and its practical implementation (i.e., what information can be shared and when) as a reason for failing to engage in information sharing:

> it's just a lack of understanding of what you can do with intelligence within GDPR now and within force guidelines (P1).

> a lack of understanding, a lack of knowledge . . . policing doesn't understand data protection. . . (P12).

> there are loads and loads and loads of missed gateways[5]. We're talking at least 70, up to 100 missed gateways. The problem is people don't use those gateways because they're worried about sharing information. This is cultural, not legislative. . . a.) they don't know about them, and b.) they think if they use them they're going to lose their job. . . This isn't about the misuse of data, it's about the missed use of data (P41).

A force data protection officer explained that constantly repeating basic advice was frustrating, especially when the circumstances varied only slightly, and the same rules applied:

> They've asked . . . effectively the same question . . . 'can I share this data?' I've looked at it and gone 'yes you can, this is your legitimate reason'. So it's almost akin to . . . 'can I tell X or Y what I had for dinner last night?' and we go 'yes you can . . . because X reason . . . '. Then . . . 'can I tell them what I had for breakfast?' and it's like 'well it's still a meal you had yesterday, so OK' . . . then the next one will be 'right they want to know what snacks I had' . . . they see each request as different, we can see they're the same (P35).

ii) *Complex legislation and bureaucratic processes*: Whilst the use of formal processes and agreements are introduced to facilitate information sharing, a sense of frustration was evident. The legislation itself was deemed to lack clarity and inhibited the ability to easily share information:

> last thing you want to do is go back and read the legislation and work out what you have got to do in trying to interpret it (P22).

> There should be a presumption to share, not a presumption to hold. This is the problem, we've got something called the 'data protection act' . . . it's got the word 'protection' in it, that was a missed opportunity, it should've been the 'data sharing act' . . . (P41).

Additionally, ISAs or MoUs were associated with bureaucracy as they required a lengthy and convoluted process. P26 commented that such processes are duplicated across all Forces within England and Wales and others noted that the problems increase with external organisations:

> External partners are absolutely crazy for information sharing agreements . . . It really is hard work. So, for each time we approach, say, an insurance company or a manufacturer to try and get them to share data with us, they want a new information sharing agreement and that has to be bespoke to them. So, it has to go through their legal department and then it has to go through our legal department (P27).

iii) *Limited training and guidance*: Participants highlighted, due to the uncertainty surrounding information sharing, access to the right guidance was important. However, it was felt the problem was compounded by a lack of relevant training and guidance, which often focused on 'what you can't do, rather than tell you what you need to do' (P22):

> I think it's a lack of training. We get guidance notes attached to legislation, but sometimes the guidance notes are so complicated and don't reflect what the legislation actually says. It just leaves a bigger loophole or a bigger 'open to interpretation' if you like (P24).

iv) *Fear and avoidance*: Participants discussed a sense of nervousness and concern of unintentionally violating legislation. This 'fear of being incorrect or wrong by genuine error in sharing' (P9) resulted in individuals being hesitant or failing to share information:

> that fear of sharing stops you from doing it . . . It's difficult because no one wants to get in trouble (P5).

This unease made legislative reasons 'very easy for people to hide behind' (P32):

> *It's one of those catchall phrases that everybody uses, isn't it . . . 'oh, we'll just say GDPR', that's it and I won't have to do anything then* (P27).

v) Support for the legislation: Not all comments were negative, and some expressed support for the legislation, arguing it provided a legal justification and 'a framework' to share information (P33):

> I think we sometimes overcomplicate it ourselves because if there is a crime purpose you can actually share data. From a policing perspective, it is quite easy (P29).

Participants added they would rather justify why they shared information (i.e., safeguarding) than explain why they did not (i.e., at a public inquiry). These practitioners also welcomed formal sharing agreements (i.e., ISAs, MoUs) as they provided the conditions to share information on a regular basis, ensuring legislative compliance and reassurance:

> police forces sign them because they're happy that they can take information from us and give information back to us because of that agreement (P1).

Stage 2: freedom of information requests

The data received in response to the FOI requests varied in timeframe, type of information and level of detail; an overview is presented to offer insight into the existing data breach landscape.

Data breaches

Table 1 shows the number of agencies who provided data for each of the years. Overall data was provided by 32 agencies, which involved a total of 28,654 data breaches.

For those who provided 2021 data ($n = 28$) their establishment levels (Home Office, 2021; Police Scotland, 2021; Police Service of Northern Ireland, 2021) were compared with the number of data breaches. A Kendall's tau correlation indicates that the larger the force (in terms of personnel numbers), the higher the number of data breaches reported, $\tau_b = .388$, $p < 0.01$.

15 agencies provided information on the type of breaches recorded. Table 2 presents a descriptive overview of all incidents provided from 2018 to 2022. Incidents of 'unauthorised access or disclosure' were recorded by most agencies, with this breach category and 'email misuse' recording the highest number of incidents. Only one incident of 'malware' was recorded by one agency.

Table 1. Data breaches: Descriptive statistics by year.

Year	n	Mean (SD)	Range	Total
2018	23	119.87 (182.95)	3–869	2757
2019	24	206.25 (293.76)	10–1343	4950
2020	27	239.78 (359.13)	1–1407	6474
2021	29	229.90 (287.91)	24–1114	6667
2022	31	189.87 (195.88)	1–777	5886
Total	**32**	**895.44 (1115.97)**	**1–4424**	**28654**

Table 2. Type of breach: Descriptive statistics.

Breach category	n (agencies)	Mean (SD)	Range	Total (incidents)
Unauthorised access or disclosure	14	269.79 (359.47)	21–1409	3777
Email misuse	11	303.45 (620.01)	1–1954	3338
Unspecified	11	231.27 (486.24)	1–1675	2544
Disclosure to incorrect recipient (via email, post, text or unspecified means)	9	131.56 (69.90)	30–206	1184
Lost or stolen devices or technological assets	11	58.27 (83.85)	1–243	641
Loss of ID or warrant cards	5	95.40 (103.20)	1–252	477
Loss of seized property	12	37.92 (39.07)	1–133	455
Data stored unsecurely/incorrectly (data integrity)	8	20.38 (32.66)	1–100	163
Failure to redact	7	23.29 (43.36)	1–120	163
Force system misuse	9	16.33 (16.75)	1–54	147
Verbal disclosure	6	14.67 (25.48)	1–66	88
Incorrect information disclosed	5	12.20 (5.12)	6–18	61
Software or system failings	10	6.10 (5.97)	1–19	61
Physical security breach	3	17.00 (21.00)	2–41	51
Cyber attacks	5	4.80 (3.90)	1–9	24
Social media misuse	1	17.00 (-)	17	17
Document misuse	2	5.50 (4.95)	2–9	11
Unsecure disposal of data	6	1.67 (1.21)	1–4	10
Device misuse	3	3.00 (2.65)	1–6	9
Lost or stolen data	4	2.25 (1.50)	1–4	9
Malware	1	1.00 (-)	1	1

ICO referrals relating to data breaches

Table 3 relates to 23 agencies who provided information about ICO referrals. Of the 18,512 data breaches recorded by these agencies, the ICO were notified about 266 breaches (1.44%).

A Kendall's tau correlation reported a significant, positive association between the total number of data breaches and the total number of ICO reports; whilst this relationship is of a moderate strength, it suggests that the higher the number of data breaches reported, the higher the number of ICO referrals, $\tau_b = .335$, $p < 0.05$.

Of the nine agencies who detailed the ICO outcome, eight stated there was no further action required or no fines received. The ninth agency did not report any punitive actions (i.e., fines), but did note the recommendations from the ICO, including: reinforcing internal procedure, ensuring all staff are suitably trained, reviewing the frequency of refresher training, conducting an internal process review, and ensuring clear guidance is available.

Discussion

The 21st Century has seen a revolution in technology and digitisation, which has transformed the way societies operate across the world. To manage the exponential growth in data, governments have implemented legislation which attempts to allow the legitimate sharing of information whilst

Table 3. ICO referrals: Descriptive statistics by year.

Year	n (agencies)	Mean (SD)	Range	Total (referrals)
2018	16	3.50 (4.87)	0–19	56
2019	16	3.38 (2.03)	1–8	54
2020	19	2.21 (2.49)	0–11	42
2021	20	2.85 (1.87)	0–6	57
2022	21	2.05 (3.07)	0–13	43
Total	**23**	**11.57 (9.07)**	**0–45**	**266**

protecting individual rights. However, international evidence shows intelligence failures continue to be commonplace and associated with tragic consequences. Faced with these issues, this research aims to understand (in greater detail) why legislation can obstruct information sharing and how this could be prevented. Whilst all developed countries have instigated data protection legislation, the UK was chosen as a practical example to focus on as it resembles data privacy principles from other countries, and mirrors (in most details) the rest of the European Union.

At the outset, the literature review showed that legislation has previously been reported as an impediment to law enforcement information sharing. It also illustrated that as the level, type and format of data has increased, data privacy legislation has evolved incrementally. This is true across the world and has resulted in data sharing rules being shaped by various laws and directives. This dictates what, when and who information can be shared with, and whether this sharing is obligatory or discretionary. Overall, the existing legal landscape is described as complex, which 'presents challenges to joint operational working' (UK Parliament, 2023, p. 12).

The first element of the mixed methods approach was to explore the views of law enforcement practitioners, who were experienced in intelligence management surrounding serious crime. They endorsed previous findings in asserting that legislation did negatively influence the effectiveness and efficiency of information sharing. However, further clarification showed this was not because of the way the laws were drafted. Participants felt many front-line operatives have a limited comprehension of data protection legislation. This was because information sharing was not treated as a strategic priority by their organisation, leading to a lack of expert guidance or training. This results in uncertainty as to what information can be shared, with who, and in what circumstances. These concerns are compounded due to the accountability structure, with practitioners voicing fears about breaching legislation and suffering a substantial sanction (Shorrock et al., 2023). In fact, the Bichard Inquiry (2004) concluded that whilst the legislation was 'inelegant and cumbersome' the problem lay more with police officers' apprehension about breaching the legislation due to a lack of education, guidance and reassurance (Bichard, 2004, p. 4). These reasons serve as valid explanations for practitioners only sharing partial information (Chan & Bennett Moses, 2017) or showing hesitancy about sharing any information at all (Plecas et al., 2011). A further important observation related to bureaucracy. As the legislation does not stipulate how implementation should take place, no universal approach exists. Practitioners explained that each organisation involved in tackling crime (which includes all public sector and many private sector organisations) interpret the legislation in their own way and generate their own protocols, processes and audit trail. This amplifies the effort and time needed to legitimately share information as new partnerships necessitate fresh negotiations and paperwork. This inconsistent and convoluted approach does not encourage information sharing.

The second stage of the study explored whether it was legitimate for practitioners to be concerned about receiving punitive sanctions, should they get it wrong. Specifically, it reviewed all data breaches registered by UK police agencies to examine whether noncompliance was commonplace, the most frequent type of breach, and the sanctions they received. However, even before the analysis was conducted the process was revealing. Individual agencies held this information in different formats, whilst some were unable to provide it. This disorganised approach supported the view that information sharing lacked strategic importance to law enforcement and detracted from the ability to learn from mistakes. Although this variation could be viewed as a limitation, methodological concerns are counteracted by interviews with experts (von Soest, 2023), as well as FOI requests being a 'powerful tool' in providing important real-world insights into the wider issue of inconsistent approaches and data management between forces (Savage & Hyde, 2014, p. 315).

For the police forces who provided data, there appeared a consistent picture. There was a correlation between the largest organisations (in terms of personnel) and the largest number of breaches. As the type and pattern of breach seemed similar across individual Forces, the increase in frequency is thought to be proportionate. The larger the organisation the more incidents they will

attend and the more data they will collate and manage. As such, larger organisations would be expected to show more breaches. Overall, the breaches themselves mainly involved unauthorised disclosures, email misuse, and disclosure to incorrect recipients. Only a small proportion of these breaches met the threshold for referral to the ICO, and none resulted in punitive measures. The likely outcome of data breaches (of those that met the ICO referral threshold) resulted in recommendations associated with training and guidance as opposed to disciplinary outcomes. This quantitative data challenges practitioner attitudes, suggesting a fear of reprisal should not be a reason for practitioners to hesitate or withhold information. This supports the finding that information sharing is not directly hindered by legislation, but rather by practitioner perceptions and attitudes towards it – at both policy and tactical level. Moreover, whilst it is not possible in this study to make a causal link between training and guidance (or lack of) and instances where a breach occurs in error, misunderstanding and/or fear, the results indicate a review of the efficacy of current training provisions may be beneficial.

The findings generally support previous findings, adding new detail and fresh insights. This is an enduring issue, with the complexity of the legal landscape and subsequent confusion surrounding legal obligations being commonly cited. This complexity is likely to grow as a) the amount of data is likely to increase, b) the data format will diversify as technology advances, c) information sharing will become increasingly required at an international level to combat criminal mobility, and d) more legislation will be required to respond to the changing environment. To combat this, and based on the analysis provided, the study generates several suggestions to improve the effectiveness and efficiency of information sharing.

First, those who draft legislation could assist greatly if they considered implementation in more detail. Providing advice surrounding what critical points practitioners should report and the level of audit required, would prevent tens of thousands of individuals duplicating effort. Secondly, at a national and multi-agency level, efforts should be made to streamline ISAs. National agreements on universal forms and processes would reduce bureaucracy as well as the effort and cost consumed by agencies and their legal departments. Third, information sharing should be valued more within law enforcement agencies as it will be of increasing value in tracking mobile criminality. Highlighting its importance would promote engagement with experts or in-agency data protection teams and make training and guidance more readily accessible. Fourth, practitioners should be reminded that legislation exists to facilitate information sharing, as opposed to hindering it, and be encouraged and empowered to share it when tackling crime. Finally, as data protection concerns can be overcome using technology, more thought should go into how integrated systems can be generated to automate information sharing within the confines of privacy legislation (Akbulut et al., 2009; Plecas et al., 2011). This would reduce bureaucracy and generally increase efficiency.

Finally, it is recognised that whilst this article has outlined the global challenges surrounding data privacy, this study is based solely on UK empirical evidence. The article has argued that the principles underpinning UK-based legislation have many similarities to other countries across the world. However, whilst the principles are transferable each country will have its nuances in terms of the legislation, culture, and organisational procedures. As such, it would be beneficial for similar research to be replicated in other countries.

Conclusion

International studies highlight the problems encountered by law enforcement agencies when sharing information. This hinders proactive and efficient policing practice, which minimises harm. Studies have previously highlighted that legislation acts as an inhibitor in information sharing and this study aims to provide more insight as to why this is the case. The evidence shows that data breaches are caused by human error and are not punitively sanctioned by governance bodies. However, practitioner interviews clearly revealed that legislation was used as a reason not to share information and there was considerable evidence to show that practitioners were

unsure of its content or deterred by the level of bureaucracy associated with the process. Changing this environment requires both strategic and tactical intervention. At a policy level, this legislative framework can be improved by considering its implementation from a user perspective. This would streamline process and reduce bureaucracy. The role of technology to provide automation and integrate systems, operating within legislative requirements, could also help in the future. Additionally, the evidence indicates that data management is increasingly a strategic priority for law enforcement, which is currently not being recognised.

Notes

1. The LED is 'for competent authorities processing for law enforcement purposes. The LED as an EU directive does not have direct effect and requires national law to implement it' (ICO, 2019, p. 4).
2. Competent authorities include chief officers of police and other policing bodies, other authorities with investigatory functions, authorities with functions relating to offender management, and other authorities (Schedule 7 of the DPA 2018), or 'any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes' (Part 3 of the DPA 2018).
3. 'The CLPD provisions extend to police forces in England and Wales. The Police Service of Northern Ireland has voluntarily adopted the CLPD provisions and separate arrangements exist within Scotland' (NPCC, 2017, p. 1).
4. However, it was not necessarily evident which breach categories they related to so they therefore remained in the data.
5. A 'gateway' refers to a statutory power or obligation to share information.
6. Categories listed, but without the number of instances.
7. No data held for breaches in 2020. Data relating to ICO reports provided for 2020–2022

Acknowledgments

The authors would like to thank all those who participated in the interviews and the agencies who responded to the FOI requests. The authors also extend their thanks to Lauren Swan-Keig for her assistance with data collection.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by a UK Research and Innovation Future Leaders Fellowship under Grant MR/V027344/1.

Notes on contributors

Becky Phythian is a Reader in Policing at Edge Hill University. She holds a UK Research and Innovation Future Leaders Fellowship exploring international law enforcement information exchange between the UK, Australia, New Zealand, USA and Canada. The project is supported by national and international partners in industry, law enforcement and academia. Previously, Becky was seconded to Lancashire Constabulary's Evidence-Based Policing Research Hub and has conducted research with various criminal justice agencies.

Stuart Kirby is a chartered psychologist and Professor Emeritus of Policing at the University of Central Lancashire. He previously served as a Detective Chief Superintendent for the Specialist Crime and Operations Division, in the Lancashire Constabulary where he had responsibility for Intelligence, Forensic, Major Crime, Organised Crime and Counter Terrorism. Stuart acts as a consultant to UK police forces and the NPCC, and has engaged with police forces across the world, including USA, India, Canada and Australia.

ORCID

Rebecca Phythian http://orcid.org/0000-0001-6423-2116
Stuart Kirby http://orcid.org/0000-0002-3049-1248

Ethics statement

The research was reviewed and approved by Edge Hill University's Social Sciences Research Ethics Committee (SSREC) (ETH2223–0295; ETH2122–0083). Informed consent was obtained from all participants.

References

Abrahamson, D. E., & Goodman-Delahunty, J. (2014). Impediments to information and knowledge sharing within policing: A study of three Canadian policing organizations. *SAGE Open*, *4*(1), 1–17. https://doi.org/10.1177/2158244013519363

Akbulut, Y. A., Kelle, P., Pawlowski, S. D., Schneider, H., & Looney, C. A. (2009). To share or not to share? Examining the factors influencing local agency electronic information sharing. *International Journal of Business Information Systems*, *4*(2), 143–172. https://doi.org/10.1504/IJBIS.2009.022821

Akbulut-Bailey, A. Y. (2011). Information sharing between local and state governments. *Journal of Computer Information Systems*, *51*(4), 53–63. https://doi.org/10.1080/08874417.2011.11645501

Bennett Moses, L. (2020). Who owns information? Law enforcement information sharing as a case study in conceptual confusion. *The University of New South Wales Law Journal*, *43*(2), 615–641. https://doi.org/10.53637/ZHNC6771

Bichard, M. (2004). *The Bichard Inquiry*. The Stationery Office. https://dera.ioe.ac.uk/id/eprint/6394/1/report.pdf

Birdi, K., Griffiths, K., Turgoose, C., Alsina, V., Andrei, D., Băban, A., Bayerl, S., Bisogni, F., Chirică, S., Costanzo, P., Fernández, C., Ficet, J., Gascó, M., Gruschinske, M., Horton, K., Jacobs, G., Jochoms, T., Krstevska, K. … Vonaş, G. (2020). Factors influencing cross-border knowledge sharing by police organisations: An integration of ten European case studies. *Police Practice & Research*, *22*(1), 3–22. https://doi.org/10.1080/15614263.2020.1789462

Blanchard, S. (2023, January). *ICO publishes reprimands not just fines. Data Protection Network*. https://dpnetwork.org.uk/ico-publishes-reprimands-not-just-fines/

Bourton, S., Ryder, N., & Brimblecombe, F. (2022). *The exchange of information and financial crime in the United Kingdom*. Synalogik. https://synalogik.com/whitepaper/when-can-government-organisations-and-law-enforcement-agencies-share-data-and-for-what-purposes

Boyne, S. M. (2018). Data Protection in the United States. *The American Journal of Comparative Law*, *66*(1), 299–343. https://doi.org/10.1093/ajcl/avy016

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021). *Thematic Analysis: A Practical Guide*. Sage.

Carter, J. G., Phillips, S. W., & Gayadeen, S. M. (2014). Implementing intelligence-led policing: An application of loose-coupling theory. *Journal of Criminal Justice*, *42*(6), 433–442. https://doi.org/10.1016/j.jcrimjus.2014.08.002

Centre of Excellence for Information Sharing. (2017). *Information Sharing to Protect Vulnerable Children and Families Programme: Strategic Meeting 24 January 2017*. https://informationsharing.org.uk/download/370/

Chan, J. (2003). Police and new technologies. In T. Newburn (Ed.), *Handbook of Policing* (pp. 655–679). Willan Publishing.

Chan, J., & Bennett Moses, L. (2017). Making sense of big data for security. *The British Journal of Criminology*, *57*(2), 299–319. https://doi.org/10.1093/bjc/azw059

Chan, J., Logan, S., & Bennett Moses, L. (2022). Rules in information sharing for security. *Criminology & Criminal Justice*, *22*(2), 304–322. https://doi.org/10.1177/1748895820960199

Chaudhury, R. D., & Choe, C. (2023). Digital Privacy: GDPR and its lessons for Australia. *Australian Economic Review*, *56*(2), 204–220. https://doi.org/10.1111/1467-8462.12506

College of Policing. (2020). *Information Sharing*. https://www.college.police.uk/app/information-management/information-sharing

Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and Conducting Mixed Methods Research*. Sage.

Department for Education. (2023). *Improving Multiagency Information Sharing: Government Policy on Information Sharing and the Use of a Consistent Child Identifier*. https://assets.publishing.service.gov.uk/media/64d500285cac65000dc2dd91/Improving_multi-agency_information_sharing_2023.pdf

Department for Education. (2024). *Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents, and Carers*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1062969/Information_sharing_advice_practitioners_safeguarding_services.pdf

Dhillon, S., & Bailey, I. (2014). *Inquiry slams police in Pickton case. The Globe and Mail*. https://www.theglobeandmail.com/news/british-columbia/inquiry-slams-police-in-pickton-case/article6477651/

Farivar, C. (2021, September 11). *20 years after 9/11, 'fusion centers' have done little to combat terrorism. NBC News*. https://www.nbcnews.com/business/business-news/20-years-after-9-11-fusion-centers-have-done-little-n1278949

Fetters, M. D., & Freshwater, D. (2015). The 1 + 1 = 3 integration challenge. *Journal of Mixed Methods Research*, *9*(2), 115–117. https://doi.org/10.1177/1558689815581222
Greenleaf, G. (2023). India's 2023 Data Privacy Act: Business/government Friendly, Consumer Hostile. *Privacy Laws and Business International Report*, *185*(1), 3–12. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4666389
Hetherington, G. (2022, June 15). *Disgraced ex-Cleveland police officer breached data laws*. *The Northern Echo*. https://www.thenorthernecho.co.uk/news/20212577.disgraced-ex-cleveland-police-officer-breached-data-laws/
Heusala, A., & Koistinen, J. (2018). 'Rules of the game' in cross-border cooperation: Legal-administrative differences in Finnish-Russian crime prevention. *International Review of Administrative Sciences*, *84*(2), 354–370. https://doi.org/10.1177/0020852315625786
Home Office. (2010). *Information Sharing for Community Safety: Guidance and Practice Advice*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97842/guidance.pdf
Home Office. (2021). *Police Workforce, England and Wales: 30 September 2021*. https://www.gov.uk/government/statistics/police-workforce-england-and-wales-30-september-2021/police-workforce-england-and-wales-30-september-2021
ICO. (n.d.-b). *Enforcement Action*. https://ico.org.uk/action-weve-taken/enforcement/
ICO (n.d.-a). *Sharing Personal Data with Law Enforcement Authorities*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/sharing-personal-data-with-law-enforcement-authorities/
ICO. (2019). *An Overview of the Data Protection Act 2018*. https://ico.org.uk/media/2614158/ico-introduction-to-the-data-protection-bill.pdf
ICO. (2022a). *Guide to Law Enforcement Processing*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/
ICO. (2022b). *ICO Sets Out Revised Approach to Public Sector Enforcement*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-sets-out-revised-approach-to-public-sector-enforcement/
Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, *1*(2), 112–133. https://doi.org/10.1177/1558689806298224
Karran, E. (2021, October 1). *Lincolnshire Police forced to pay out £10k after PC's illegal data breach*. *The Lincolnite*. https://thelincolnite.co.uk/2021/10/lincolnshire-police-forced-to-pay-out-10k-after-pcs-illegal-data-breach/
Kirby, S. (2013). *Police effectiveness: Implementation in theory and practice*. Palgrave MacMillan.
Legal Expert. (2022). *Police Force Data Breaches: An analysis of Freedom of Information requests*. https://www.legalexpert.co.uk/wp-content/uploads/2022/08/legal-expert-police-data-breach-report-2022.pdf
MacAlister, J. (2022). *The Independent Review of Children's Social Care: Final Report*. Department for Education. https://webarchive.nationalarchives.gov.uk/ukgwa/20230308122535mp_/https://childrenssocialcare.independent-review.uk/wp-content/uploads/2022/05/The-independent-review-of-childrens-social-care-Final-report.pdf
Monaghan, P., Waring, S., Giles, S., & O'Brien, F. (2024). What works in improving inter-agency responses to missing children investigations: A scoping review. *The Police Journal*, https://doi.org/10.1177/0032258X241241016
Mouzakiti, F. (2020). Cooperation between Financial Intelligence Units in the EU: Stuck in the middle between the GDPR and the Police Data Protective Directive. *New Journal of European Criminal Law*, *11*(3), 351–374. https://doi.org/10.1177/2032284420943303
National Police Chiefs' Council. (2017). *Common Law Police Disclosures*. https://assets.production.copweb.aws.college.police.uk/s3fs-public/2022-04/NPCC-2017-Common-Law-Police-Disclosures-CLPD-%E2%80%93-Provisions-to-supersede-the-Notifiable-Occupations-Scheme-NOS.pdf
Nooteboom, B. (2003). The trust process. In B. Nooteboom & F. Six (Eds.), *The Trust Process in Organizations: Empirical Studies of Determinants and the Process of Trust Development* (pp. 16–36). Edward Elgar.
Peel, M., & Rowley, J. (2010). Information sharing practice in multi-agency working. *Aslib Proceedings: New Information Perspectives*, *62*(1), 11–28. https://doi.org/10.1108/00012531011015172
Peters, G. (2023). *Planned in Plain Sight: A review of the intelligence failures in advance of January 6th, 2021*. Committee on Homeland Security and Governmental Affairs. https://www.hsgac.senate.gov/wp-content/uploads/230627_HSGAC-Majority-Report_Jan-6-Intel.pdf
Phythian, R., & Kirby, S. (2022). What does the UK Police National Database tell us about the future of police intelligence? *Policing: A Journal of Policy and Practice*, *17*, 1–14. https://doi.org/10.1093/police/paac074
Plecas, D., McCormick, A., Levine, V., Neal, J. P., & Cohen, I. M. (2011). Evidence-based solution to information sharing between law enforcement agencies. *Policing an International Journal*, *34*(1), 120–134. https://doi.org/10.1108/13639511111106641
Police Scotland. (2021). *Police Scotland Officer's & Staff Quarterly Fact Sheets: Quarter 3 - 30/09/2021*. https://www.scotland.police.uk/about-us/how-we-do-it/police-scotland-officer-numbers/
Police Service of Northern Ireland. (2021). Freedom of Information request: PSNI Police Officer Diversity. https://www.psni.police.uk/sites/default/files/2022-09/01799%20Police%20Officer%20Diversity.pdf
RUSI. (2023). *A boundless threat? The rise of organised crime in the UK*. https://www.rusi.org/explore-our-research/publications/commentary/boundless-threat-rise-organised-crime-uk
Savage, A., & Hyde, R. (2014). Using freedom of information requests to facilitate research. *International Journal of Social Research Methodology*, *17*(3), 303–317. https://doi.org/10.1080/13645579.2012.742280

Shorrock, S., Parker, S., Addidle, G., M, M., Liddle, J., Martin, D., Proctor, T., & Olive, P. (2023). Standardising multi-agency safeguarding hubs (MASH): Building a framework to effectively identify and manage risk. *Emerald Open Research*, *1*(13). https://doi.org/10.1108/EOR-13-2023-0022

Sidebotham, P., Brandon, M., Bailey, S., Belderson, P., Dodsworth, J., Garstang, J., Harrison, E., Retzer, A., & Sorensen, P. (2016). *Pathways to harm, pathways to protection: A triennial analysis of serious case reviews 2011 to 2014*. Department for Education. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/533826/Triennial_Analysis_of_SCRs_2011-2014_-__Pathways_to_harm_and_protection.pdf

Skinns, L. (2023). Researching inside police custody in four jurisdictions: 'Getting in', 'getting on', 'getting your hands dirty' and 'getting through it'. *Criminology & Criminal Justice*, *23*(2), 273–289. https://doi.org/10.1177/17488958221087491

Todak, N., & Somers, L. J. (2024). A tutorial on mixed methods research for policing scholars. *The Police Journal*, https://doi.org/10.1177/0032258X241299749

Treiber, A., Müllmann, D., Schneider, T., & Döhmann Spiecker Genannt, I. (2022). Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies. *WPES'22: Proceedings of the 21st Workshop on Privacy in the Electronic Society* (pp. 69–82). https://doi.org/10.1145/3559613.3563192

UK Parliament. (2023). *Data Protection and Digital Information Bill: Explanatory Notes*. https://bills.parliament.uk/publications/53323/documents/4144

United Nations Conference on Trade and Development. (2025). *Data Protection and Privacy Worldwide*. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

von Soest, C. (2023). Why do we speak to experts? Reviving the strength of the expert interview method. *Perspectives on Politics*, *21*(1), 277–287. https://doi.org/10.1017/S1537592722001116

Waring, S., Taylor, E., Giles, S., Almond, L., & Gidman, V. (2022). "Dare to Share": Improving information sharing and risk assessment in multiteam systems managing offender probation. *Frontiers in Psychology*, *13*, 1–13. https://doi.org/10.3389/fpsyg.2022.869673

Williams, W. (1982). *Studying Implementation: Methodological and Administrative Issues*. Chatham House Publishers.

Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, *3*(6). https://doi.org/10.1007/s44216-024-00028-2

Appendices

Under **the Freedom of Information Act 2000** I would like to request the following information: The number of data breaches reported to your force data protection officer, or equivalent, for each of the following years:

1. 2018
2. 2019
3. 2020
4. 2021
5. 2022

Please provide a breakdown for each year including:
i) the month/year of the breach
ii) a summary of the nature of the breach including a description of the data involved, including whose data it was compromised, e.g., Police officer/civilian employee, members of the public, witnesses etc.
iii) details of the circumstance of the breach and any subsequent risks arising from the breach
iv) whether or not the breach was reported to the Information Commissioner Office (ICO) and what the repercussions of that was, i.e., any fines from the ICO.

Figure A1. Freedom of Information (FOI) request.

Initial FOI requests (n=49)

47 agencies responded within the data collection period:

- 19 provided information: the NPCC also returned data for ACRO Criminal Records Office, and one force provided an unclear dataset but did not respond to requests for clarification resulting in its exclusion.
- 28 refused the request: 26 quoted S.12 of the FOI Act (2000) (the cost of compliance exceeds the appropriate limit) and two quoted both S.24 (safeguarding national security) and S.31 (disclosure would be likely to prejudice).

↓

Refined FOI requests (n=28)

Requests were refined based on the agency's reason for refusal (e.g. reducing the time frame) and resubmitted:

- 13 agencies returned data.
- 15 maintained their refusal: 14 quoted S.12, and one quoted both S.24 and S.31. Nine also stated an inability to supply datasets due to information being held on multiple databases.

↓

Data provided (n=32)

Reasons for providing limited datasets included: S.12 (n=13); S.14 (dealing with vexatious requests) (n=1); S.24 (n= 6); S.31 (n=8); S.40 (personal information) (n=2) and S.41 (information provided in confidence) (n=1).

Figure A2. Overview of FOI request process.

Table A1. An overview of the data provided by each agency.

Agency	Timeframe	Number of breaches	Type of breach	ICO referral
ACRO	01/18–09/22	Count per month	–	–
Avon and Somerset Constabulary	06/18–12/22	Count per month	–	–
Cheshire Constabulary	01/01/18–06/12/22	Count per year	–	Number of reports and fines
City of London Police	Unspecified	Summary of one offence	Summary	If reported
Civil Nuclear Constabulary	06/03/18–21/11/22	Incident-by-incident	Summary	Date reported
Cleveland Police	12/20–12/22	Incident-by-incident	Summary	If reported
Cumbria Constabulary	01/01/18–25/11/22	Count per year	–	Total number reported
Derbyshire Constabulary	10/01/18–09/12/22	Incident-by-incident	Category	Date reported
Devon and Cornwall Constabulary	2018–09/12/22	Count per year	Category	–
Durham Constabulary	2018–26/11/22	Count per year	–[6]	Number of reports and fines
Gwent Police	04/05/18–07/12/22	Incident-by-incident	Summary	If reported and outcome
Humberside Police	2020 – 2022	Count per year	Category	–
Kent Police	01/18–11/22	Count per month	Category	Number of reports
Lancashire Constabulary	2018–2022	5 year total	Category	–
Leicestershire Constabulary	01/18–12/22	Count per month	-[5]	Number of reports
Lincolnshire Police	25/04/18–20/12/22	Incident-by-incident	Summary	If reported and outcome
Merseyside Police	2019 – 2022	Count per quarter	–	–
National Police Chief's Council	2022	Count per month	–	–
North Wales Police	02/18–11/22	Incident-by-incident	Category	If reported and outcome
North Yorkshire Police	05/18–11/22	Count per year (by month for 21–22)	–	–
Northumbria Police	11/20–2022	Count per year	–	Total number reported
Nottinghamshire Police	09/18–11/22	Count per month	–	Number of reports
Police Scotland	2018 – 2022	Count per year	Category	Number of reports and outcome
Police Service of Northern Ireland	01/21–11/22	Count per month	–	Number of reports and outcome
South Wales Police	11/20–11/22	Count per month	–	Number of reports
South Yorkshire Police	09/18–01/19; 2021–05/12/22[7]	Count per year	–	Number of reports and fines
Staffordshire Police	02/18–17/11/22	Count per month	Summary	Number of reports
Surrey Police	10/01/18–10/12/22	Incident-by-incident	–	If reported
Sussex Police	2018 – 2022	Count per year	Category	Summary of report and outcome
Thames Valley Police	04/18–11/22	Count per month	–	Number of reports
West Midlands Police	06/18–11/22	Incident-by-incident	Category	If reported
Wiltshire Police	2018 – 2022	Count per year	–	–

Table A2. FOI Data: Coding dictionary for breach categories.

Breach category	Description (based on Legal Expert (2022) categories and data provided)	Categories present, or examples of content provided, in force data
Cyber attacks	A deliberate attempt to gain unauthorised access to computer systems and networks to expose, modify or steal data.	Cyber attack; cyber breach; cyber incident; malicious code
Data stored unsecurely/ incorrectly (data integrity)	Personal data that is not securely or correctly stored, such as leaving it in a place where it may be wrongly disposed of or possibly stolen.	Data integrity; data storage; data added to incorrect record; records located on clearing of premises
Device misuse	When a device is used without permission or used for a different purpose than it is intended. It may include computer misuse or unauthorised access to hard disks.	Computer misuse; images of police systems saved on a personal device; unauthorised recording of police data on a personal device
Disclosure to incorrect recipient (via email, post, text or unspecified means)	Sending information to the wrong person, whether internally or externally, either by email, post, text message or other means. This may include accidentally copying incorrect recipients into email exchanges, posting information to the wrong address or sending a text message to an incorrect phone number.	Email/document/letter/text sent to wrong recipient; bail notice sent to wrong address; records sent to incorrect address; charge sheets given to wrong recipient
Document misuse	Unauthorised access to documents and may lead to personal data being tampered with, destroyed or stolen.	Incorrectly handled paperwork; work related documents taken to their home address
Email misuse	When email accounts are accessed or used without permission and may lead to incorrect information being sent out or the wrong recipients receiving confidential information. This type of incident may involve emails being sent on unsecure servers, sensitive content being sent via unsecure means, or emails being sent in error.	Email misuse; Emailing wrong data to another force; Official Sensitive attachment sent to a trusted partner outside the secure network; sensitive document attached to meeting invite and sent to external party; accidental email disclosure to partner agency via paste of unrelated content
Failure to redact	Documents are redacted to protect information that is considered confidential. This breach occurred when information that should have been redacted before sharing was not.	Failure to redact; poorly redacted document disclosed via CPS; unredacted first name disclosed to LA; disclosure – redaction; incorrectly sanitised data sent to third party agency
Force system misuse	The use of force computer systems without consent or for reasons other than work.	System misuse; system access without legitimate purpose; third party agency accessing police system without legitimate purpose; misuse of police systems
Incorrect information disclosed	Disclosure of the incorrect information.	Incorrect information shared re: subject [NAME]; Incorrect PNC information disclosed
Loss of ID or warrant cards	The loss of ID or warrant cards, which risks others impersonating police officers creating subsequent risks to public safety and force reputation.	Lost ID; loss of ID card, warrant card etc.; ID cards/keys/warrants lost
Loss of seized property	The loss of property that is seized, or found, by police officers.	Mobile phone returned to wrong person; loss/ theft of seized/recovered/found property
Lost or stolen data	Data (e.g., paperwork) that is lost or stolen	Loss of paperwork; lost files; misplaced evidence; missing pocket book; data theft
Lost or stolen devices or technological assets	Assets (e.g., laptops, hard drives, body worn video cameras) that are lost or stolen.	Loss or Theft of Technology Assets; missing disk; theft of police laptop and notebook; lost encrypted USB stick
Malware	Software that is designed to attach computer devices and networks.	Potential malware on police terminal
Physical security breach	When outsiders from the force, or staff without appropriate access, access areas that they do not have authorised access to.	Physical security breach; Unauthorised Persons on Premises; Unsecure door
Social media misuse	Failure to uphold standards of professional behaviour on social media.	Social media; Social media – Disclosure; Social media – Document; Social media – Photo

(*Continued*)

Table A2. (Continued).

Breach category	Description (based on Legal Expert (2022) categories and data provided)	Categories present, or examples of content provided, in force data
Software or system failings	Failure to update and/or secure systems or software to avoid them failing and being at risk to unauthorised access.	ADACS system now shows user's name rather than collar number; Technical Safeguard Failure; system failure outage; system issues
Unauthorised access or disclosure	Unauthorised access to or disclosure of information	Unauthorised Disclosure; Unauthorised Access to Systems or Data; details disclosed in error; excessive information shared
Unsecure disposal of data	Failure to securely dispose of data, which risks data being accessed by unauthorised parties.	Insecure disposal of paperwork; Sensitive Information Disposed Incorrectly; disks placed into a skip
Unspecified	This category was applied if the existing category or qualitative content did not clearly fall into one of the revised categories.	Complaint from [NAME]; MFSS car hire name error; Other; Dyslexia Referral Form; fusion; data breach – voicemail; experience reports [NAMES]; airwave incident; paper document; procedural concerns; vetting personnel; Athena; biometrics; BWV; CPS; disk; document; data protection
Verbal disclosure	The verbal disclosure of personal information to someone not authorised to hear it. This could occur if an officer is overheard talking about personal information.	Verbal disclosure; Disclosure – Telephone; Disclosure – Verbal; Verbal; Call taker disclosed information over the phone; Member of the public overheard an officer pass information over their radio; Excessive information disclosed to a third party verbally