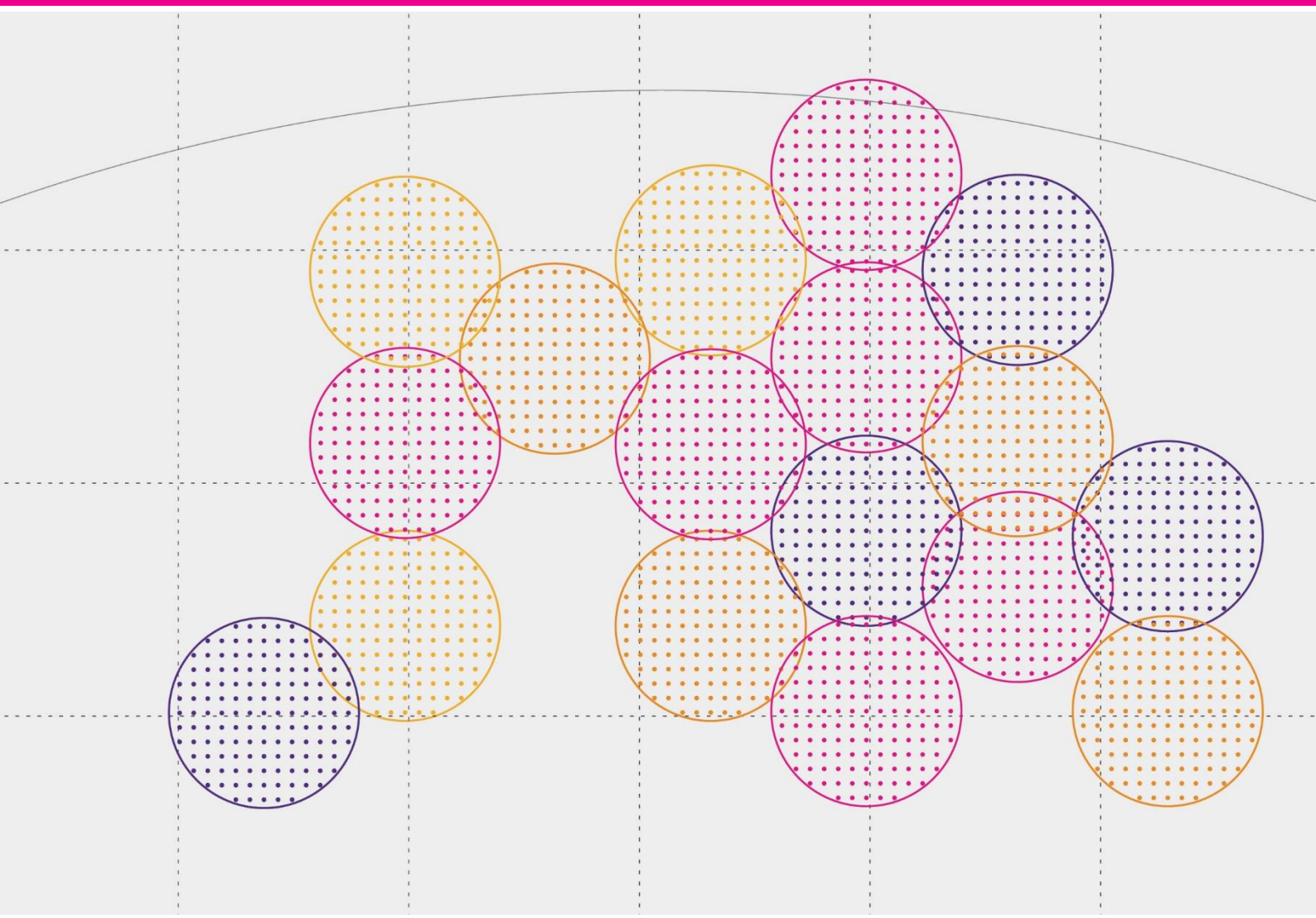
Review of literature relevant to data protection harms

March 2022

Sam Wood, Laura Wilkinson, Akhiljeet Kaur, Aude Schoentgen, Tony Lavender



plumconsulting.co.uk

About Plum

Plum is an independent consulting firm, focused on the telecommunications, media, technology, and adjacent sectors. We apply extensive industry knowledge, consulting experience, and rigorous analysis to address challenges and opportunities across regulatory, radio spectrum, economic, commercial, and technology domains.

About this study

The Information Commissioner's Office (ICO) has commissioned Plum to carry out a review of existing literature relevant to data protection harms.

Plum Consulting
10 Fitzroy Square
London
W1T 5HP

T +44 20 7047 1919
E info@plumconsulting.co.uk

Contents

Summary

Background

Data protection harms can arise through the use or misuse, or loss of personal data, or from an inability to effectively exercise data rights. Data protection harms may have a variety of impacts on individuals, ranging from financial loss, emotional distress and even physical harm. They may also have an impact on society as a whole, including on judicial and democratic processes. However, the risk of these harms occurring, and the severity of the impact, are not always well understood.

In the UK, the Information Commissioner's Office (ICO) has responsibility for promoting and enforcing data protection law. The ICO has commissioned Plum Consulting to carry out a review of existing literature relevant to data protection harms. This is intended to inform the ICO's future work to better understand the risks, severity and impacts of data protection harms, both to individuals and society as a whole.

Objectives

We worked with the ICO study team to develop the primary and secondary objectives for this review. The primary objective of the review is to:

> *Review existing evidence relevant to data protection harms, including evidence of awareness, risk and experience of individual and societal data protection harms.*

In addition, two secondary objectives were identified:

> *Identify areas where there are gaps in the evidence of data protection harms, and areas where the evidence is less robust.*
>
> *Assess the evidence around the relative risk and severity of actual and perceived harms.*

We undertook a systematic literature search across multiple sources, assessing both published and grey literature. We then screened the references collected for relevance to the primary and secondary objectives of the review. This was a two-stage process involving abstract and full text review. The study team was additionally required to organise the literature found within the ICO's taxonomy of data protection harms.

Findings

In total 111 references were eligible for the review. Some key findings from the review are set out below.

- The evidence found in our review come from a range of disciplines – including sociology, healthcare, marketing, information technology, economics, and law. This indicates that a range of sectors are considering this issue.
- The evidence found primarily focuses on the US, UK and EU jurisdictions. In the US, articles from law journals formed a key part of the evidence base. In the UK and EU, grey literature is an important source of evidence, but there are key contributions from the fields of cybersecurity and sociology.
- A range of studies assess individuals' awareness and concerns about data protection harms. In general, individuals express concern over the use of their personal data and say privacy is important to them. In particular, individuals express high levels of concern about loss of financial data or online fraud. However, outside of financial harms, their awareness of specific harms that may result from a breach of their personal data appears to be limited.

- The risks of certain types of data protection harms occurring does not appear to have been explored in a systematic manner. This is likely to reflect the challenge in linking a specific data event (such as a data breach, or the act of sharing data with a digital service) to a subsequent harm, which may occur months or years later.
- Whilst some harms are relatively well explored in empirical studies, such as loss of personal data, unwarranted intrusion and chilling effects, other harms have limited empirical evidence. For example, no empirical studies assess damage to law and justice. There are evidence gaps for harms that are otherwise well explored in the theoretical literature such as discrimination and loss of confidentiality.
- Surveys generally ask about individuals' views, concerns, or perceptions of harms, rather than experiences. However, some surveys ask individuals whether they have experienced data protection harms. In general, the proportion who report awareness of experiencing harms is substantially lower than the proportion expressing concerns (though it should be noted that some individuals may not be aware they have experienced data protection harms).
- The evidence generally supports the idea of a mismatch between individuals' reported concerns about use of personal data and their actions and behaviours (sometimes termed the 'privacy paradox'). This is variously attributed to information asymmetries, the transaction costs associated with evaluating the costs and benefits of disclosing personal data, or a sense of 'digital resignation' and 'digital fatalism'.
- A variety of studies discuss or explore the potential impacts and implications of a particular type of harm occurring (e.g. fraud or identity theft). No study in the review has attempted to explicitly quantify the impact of a particular data protection harm at an aggregate level. However, a number of studies have attempted to quantify the value individuals place on different types of personal data (e.g. the payment users are willing to accept to permit use of their data).

Mapping the literature to the ICO's taxonomy

In the process of mapping the literature to the ICO's harms taxonomy, we drew out some further findings.

- "Chilling effects" (a reduction in the use of services or activities due to an actual or perceived risk of potential harm) appears to be an area increasingly explored in the literature.
- "Discrimination" is also a relatively well-explored area in the literature, but this is largely driven by studies on price discrimination. Quantitative evidence in this area is relatively lacking.
- No study in our review dealt primarily with physical harms related to data protection. While a number of studies mentioned such harm and discussed how it might arise, they did not include estimates of prevalence.
- While acknowledging that violation of privacy is itself an impingement of an individual's rights, few studies explored the knock-on effects on other rights and freedoms. One example of where this *is* explored is in relation to ex-offenders and discrimination, where privacy violations may impact ex-offenders' rights not to disclose a spent conviction.
- Societal harms are not well-explored in general. In particular, we did not find any studies that considered harms to the environment associated with data protection issues. However:
  - some studies have explored harm to the economy that may arise as a result of unequal access to data among market players; and
  - some studies have explored the impact of voter microtargeting on the democratic process.

1 Background

The modern digital economy is underpinned by the collection and analysis of vast amounts of data. These data are used to target, refine and optimise digital services. Such services have produced enormous benefits for society and for the economy over the past decades. However, this has been accompanied by growing concerns about the consequences of use of data (including misuse and loss) and inability to exercise data rights, which may harm individuals and society as a whole.

In the UK, the Information Commissioner's Office (ICO) has responsibility for promoting and enforcing data protection law. The Information Commissioner is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. As such, it has a specific interest in understanding data protection harms.

However, harms relating to data protection can be challenging to assess and analyse. Such harms:

- are often intangible;
- are probabilistic and often intertemporal in nature;
- are often only significant in aggregate;
- may vary by data subject; and
- may be difficult to observe and avoid.

The ICO commissioned Plum Consulting (Plum) to carry out a review of existing literature relevant to data protection harms. This study has been commissioned in order to support ongoing work to inform internal and external policy-making and the prioritisation of data protection issues. The ICO is currently developing a framework to categorise harms, and to better understand the risks and severity of data protection harms affecting both individuals and society as a whole.

The purpose of this study is to build on the ICO's initial work by developing a formal evidence base. This includes both theoretical and empirical evidence relevant to the ICO's taxonomy of data protection harms and the wider scope of the study.

The findings of this study are intended to inform the ICO's future work – to better understand risks, severity and impact of data protection harms. Specifically, this should identify evidence gaps that may be addressed by further market research (i.e., to develop empirical evidence base) or theoretical research (i.e., opportunities for ICO thought-leadership) in specific areas.

At the outset of the study, the ICO specified several key focus areas and research objectives. The ICO and Plum study team then distilled these into primary and secondary study objectives, set out in Section 2.

2 Objectives of the study

The objective of this study is to enable the ICO to better understand harms relating to data protection through a review of existing literature. This will build on the ICO's initial work on data protection harms by developing a formal evidence base. In turn, this will inform future work to better understand risks, severity and impact of data protection harms, and where there are gaps in the available evidence.

The literature review is intended to collate:

- evidence on the awareness, experience of and concern about relevant data protection related harms and examples of harms identified in the literature; and
- relevant insights that could help the ICO to better understand the risk and severity of the harms identified.

We worked with the ICO study team to develop the primary and secondary objectives for this review.

The primary objective of the review is to:

> *Review existing evidence relevant to data protection harms, including evidence of awareness, risk and experience of individual and societal data protection harms.*

In addition, two secondary objectives were identified:

> *Identify areas where there are gaps in the evidence of data protection harms, and areas where the evidence is less robust.*
>
> *Assess the evidence around the relative risk and severity of actual and perceived harms.*

The secondary objectives were addressed using evidence collated from the primary searches.

The review was intended to cover both academic and grey literature (i.e. any information that is not produced by commercial publishers). The research prioritised literature set in the UK context, or in jurisdictions similar to the UK. As part of the review, we also examined data protection authorities from several key jurisdictions.

The study team was additionally required to organise the literature found within the ICO's taxonomy of data protection harms (refer to Appendix B). This was to help identify any areas where there is potential to expand or amend the ICO's taxonomy.

3 Methods and search strategy

3.1 Inclusion criteria

Relevant studies to be included were those which analyse data protection harms to individuals and society. As detailed in the research objectives, this covers various dimensions, including awareness of data protection harms, the risks and severity of harms, and individuals' experience of harms. The scope of the review included both qualitative and quantitative studies.

The scope of the review is not restricted to the UK, however greater emphasis was placed on evidence from the UK and jurisdictions similar to the UK (Europe, Australia and New Zealand) and jurisdictions where there is a relatively substantial evidence base (USA).

The review focused on studies published since 2010 in the review, with increased focus on more recent evidence.

The evidence review was undertaken over a four month period and conducted in two phases.

- Phase 1: Evidence gathering and high-level review to identify in-scope papers, conducted in late November and December 2021.
- Phase 2: In-depth review of compiled evidence, summaries and synthesis of findings, compiled in January and February 2022.

Three additional references were highlighted by the ICO in February 2022.[1,2] These were subsequently reviewed by the Plum study team and incorporated into Phase 2 analysis.

3.2 Methodology

3.2.1 Search sources

The review was undertaken using multiple information sources, intended to capture evidence from both the academic and grey literature. The sources used are listed in Figure 3.1.

Figure 3.1: Search sources for the review

Source	Description
EBSCO	EBSCO Information Services offers access to around 7,000 peer-reviewed academic journals in full text.
JSTOR	JSTOR is a digital library of academic journals, books, and primary sources, with access to over 2,600 journals.

[1] Jacob Leon Kröger, Milagros Miceli and Florian Müller, 2021. How Data Can Be Used Against People: A Classification of Personal Data Misuses. Preprint copy, 30 December 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3887097&s=03 [Kröger et al, 2021]

[2] Digital Action, 2022. DRAFT: Digital Action's online harms taxonomy. https://docs.google.com/document/d/1MPMkdxrzrNtZUIFDFFg5CKQJPTgfjNGMI1MexByJvUY/edit# [Digital Action, 2022a] and Digital Action, 2022. DRAFT: Digital Action's tech accountability policy taxonomy. https://docs.google.com/document/d/1heKZV2XN73zd3aGxoOf_vVU4veO5FkLr16Kq5XDzvfM/edit#heading=h.f56m4w4wu7s9 [Digital Action, 2022b].

Source	Description
SSRN	SSRN is an open access research platform used to share early-stage research. SSRN provides a space for a variety of content types to be accessed beyond the traditional research article, including grey literature, book reviews, multimedia files, and datasets.
Google Scholar	A search engine focused on scholarly literature.
Google	A general search engine, used to identify grey literature.
Organisation websites	As agreed with the ICO study team, we reviewed the websites of a number of relevant organisations. These included: ICO, DCMS, Ofcom, ODI, CMA, Which?, Centre for Data Ethics and Innovation, Doteveryone, Data Justice Labs, LSE Department for Media and Communications, ENISA.

3.2.2 Search terms

In discussion with the ICO study team, we prepared a set of keywords to test, in order to formulate the search strategy. These are presented in Figure 3.2.

Figure 3.2: Keywords and qualifier terms tested in developing the search strategy

Data protection keywords	Harms keywords	Qualifier keywords
Data protection	Harm	Individual
Data security	Risk	Societal
Privacy	Awareness	Financial
Data privacy	Experience	Emotional
Personal data	Impact	Economic
Personal information	Abuse	Environmental
		Loss of control
		Rights
		Discrimination

It was noted that in-scope publications typically contain one or more of the data protection keywords in the publication title. However, of these terms, "privacy" brought in a lot of out-of-scope results. For instance, there are numerous articles that examine the interpretation and implementation of the General Data Protection Regulation (GDPR), but which do not explore the topic of data protection harms. Instead, requiring privacy to appear in conjunction with "data" or "harm" generated more relevant results.

The combinations of search terms used are detailed in Section 3.2.3. Search terms were combined using a Boolean AND operator.[3]

Qualifier keywords [Individual/Societal/Financial/Emotional/Economic/Environmental/Loss of control/Rights/Discrimination] were used to illustrate areas where there may be less evidence, and incorporated into the search strategy for some search sources.

[3] Refer to: https://support.jstor.org/hc/en-us/articles/115004733187-Searching-Boolean-Operators

3.2.3 Search strategy

As our search sources offered varying levels of control over the searches, we adopted a differentiated strategy across the sources. This is presented in Figure 3.3.

Figure 3.3: Search strategy by search source.

Source	Search strategy
EBSCO	Title/body text keyword search
JSTOR	Title/body text keyword search
SSRN	Search on Data Privacy Harm* and Data Protection Harm*
Google Scholar	Run series of searches including qualifier terms, cap the number of search terms analysed
Google	Run series of searches including qualifier terms, cap the number of search terms analysed
Organisation websites†	Browse site, run site search on Data Privacy Harm* and Data Protection Harm*

We also ruled out restricting searches to certain journals. Relevant papers appear across multiple fields, including legal, sociological, economics, marketing and healthcare journals.

For our primary academic sources, we conducted title searches on our data protection keywords, but also required the term "harm" to appear in the full publication text (Figure 3.4). All results generated by these searches were captured and analysed. We also ran additional searches requiring the qualifier keywords to appear in the publication text.

Figure 3.4: Search queries for JSTOR and EBSCO

Title contains:	AND full text contains:
"data protection" OR "data security" OR "personal data" OR "personal information" OR (privacy AND data OR harm)	harm
"data protection" OR "data security" OR "personal data" OR "personal information" OR (privacy AND data OR harm)	harm

SSRN does not allow a similar combination of title and full text searching. Instead we conducted a full text search for Data Privacy Harm* and Data Protection Harm*. All results generated by these searches were captured and analysed.

For Google and Google Scholar we carried out text searches, restricting the results to items with document formats (.pdf, .doc, .docx). We conducted a number of searches using the various qualifier keywords to capture a range of evidence. Due to the large number of results generated, we capped the number of results we analysed from each search at 20 per search (or 50 for the search without a qualifier term).

Figure 3.5: Search queries for Google and Google Scholar

Text contains	AND:	AND:	Results analysed
"data protection" OR "data security" OR "personal data" OR "personal information" OR (privacy AND (data))	harm		50
	harm	Risk	20
	harm	Awareness	20
	harm	Experience	20
	harm	Impact	20
	harm	Abuse	20
	harm	Individual	20
	harm	Societal	20
	harm	Financial	20
	harm	Emotional	20
	harm	Economic	20
	harm	Environmental	20
	harm	"Loss of control"	20
	harm	Rights	20
	harm	Discrimination	20

For the organisations known to be active in this area, we used a number of methods. Firstly, we browsed the website for relevant research and information. If the website had a search function, we searched on the terms Data Privacy Harm* and Data Protection Harm*. If the website did not have a search function, we used Google site search to carry out the same searches.

Further details on the search strategy for each search source, including search date and number of relevant records identified, are set out in Appendix A.

3.3 Review screening

The first step of the review screening was completed in November and December 2021.

The results of all the searches were captured and collated into a single library. Duplicate entries were reviewed by the team and removed or merged.

The study team then reviewed the abstracts of the references found against the inclusion criteria. References that did not meet those criteria based on abstract screening were excluded from the review. To reduce subjectivity, each abstract was reviewed by two team members.

The second step of the review screening was conducted in January and February 2022.

This step involved screening the remaining references against the inclusion criteria based on a full text review. We were able to obtain the full text for all references save one – a book which we subsequently ordered from a retailer.

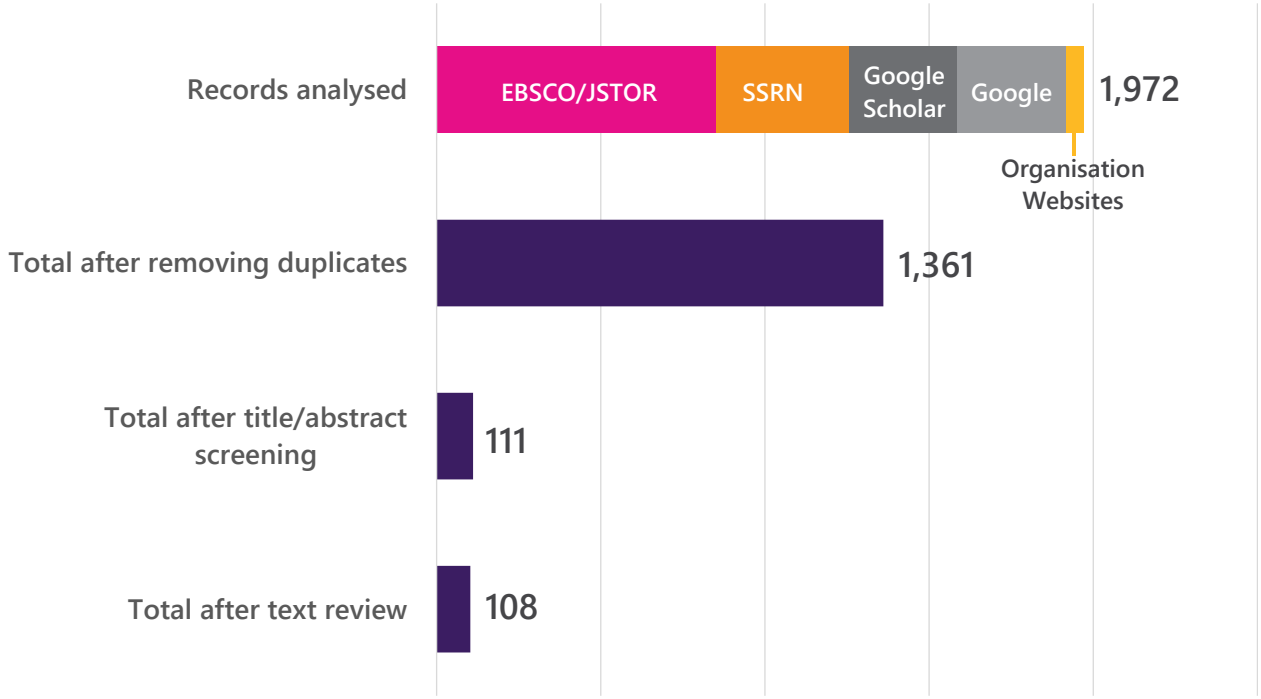
The references were categorised according to the methodology used, the jurisdiction of focus, and whether the reference focused on a particular group of individuals. References were also tagged according to the ICO's data protection harms taxonomy (refer to Section 4.3 for details). All references, along with our categorisations and tags, were exported into a Microsoft Excel file.

4 Search results

4.1 Results

The study team analysed nearly 2,000 references in carrying out the search strategy. The number of references included and excluded at each stage of the screening process is detailed in Figure 4.1.

Figure 4.1: Results of the search and screening process



Note: excludes three additional papers highlighted by ICO for inclusion in February 2022.

The majority of material found in the searches was not relevant to the primary or secondary objectives of the review. In total 108 references were judged by the study team to be relevant to the review.

Around one quarter of the references in scope were found to be from the grey literature. These were from both UK-based organisations (e.g. Ofcom, Which?, CMA) and international organisations (e.g. ENISA, OECD, Cisco).

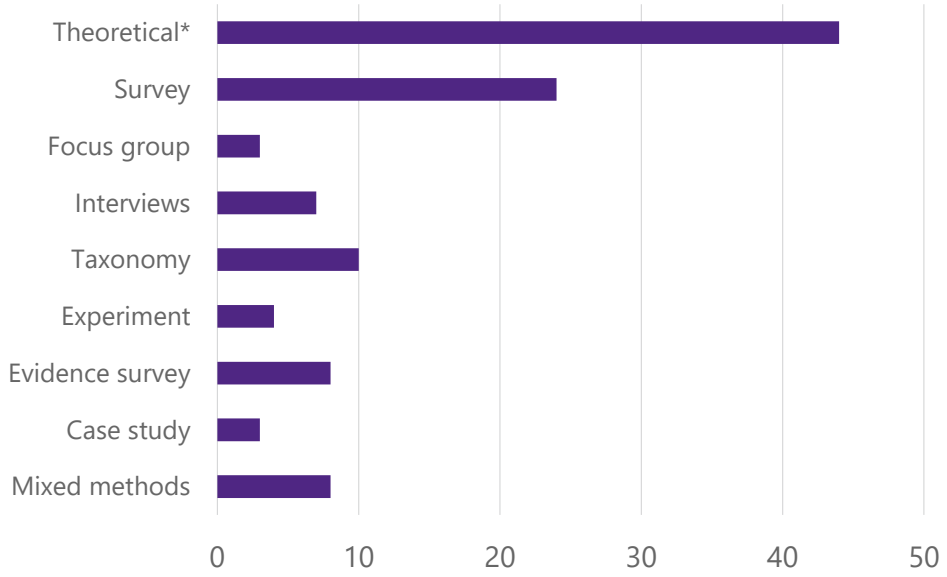
Three additional references were provided by the ICO for inclusion in February 2022, as noted in Section 3.1. Thus, a total 111 references were relevant to the scope and analysed within the review statistics below.

4.2 Review statistics

We catalogued the references in scope according to the research methodology employed (Figure 4.2). Many studies did not undertake novel primary research into data protection harms, instead discussing such harms at a conceptual level (albeit often illustrated with examples). We also identified several studies where the authors attempted to develop a taxonomy of data protection harms.

Of the studies that undertook novel primary research, surveys were the most common research method employed. Several studies used a combination of primary research methods – typically, a survey and interviews (listed as "mixed methods").

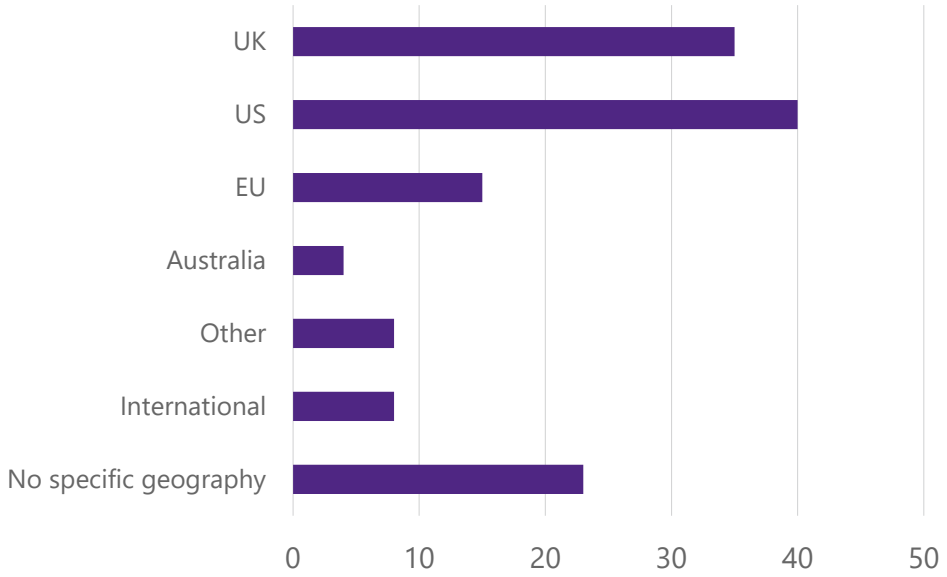
Figure 4.2: Main research methodology employed



* Theoretical used to denote when no specific primary research techniques were employed in the study. Does not include studies which develop a taxonomy.

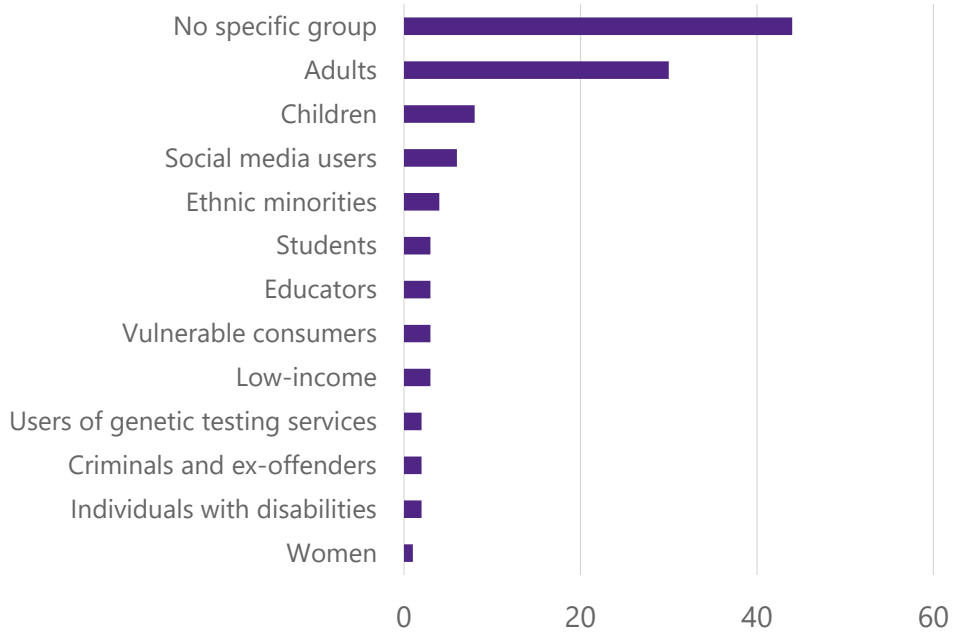
We also catalogued studies according to the jurisdiction(s) they focused on (Figure 4.3). The majority of studies focused on the US or UK. Note that some studies did not have a particular jurisdiction of focus.

Figure 4.3: Jurisdiction of focus



In addition, we also catalogued the studies according to whether they focused on a particular group (Figure 4.4). Many studies did not make reference to a particular group. Surveys tended to survey adults; however we did find a number of studies that focused on certain groups.

Figure 4.4: Groups studied

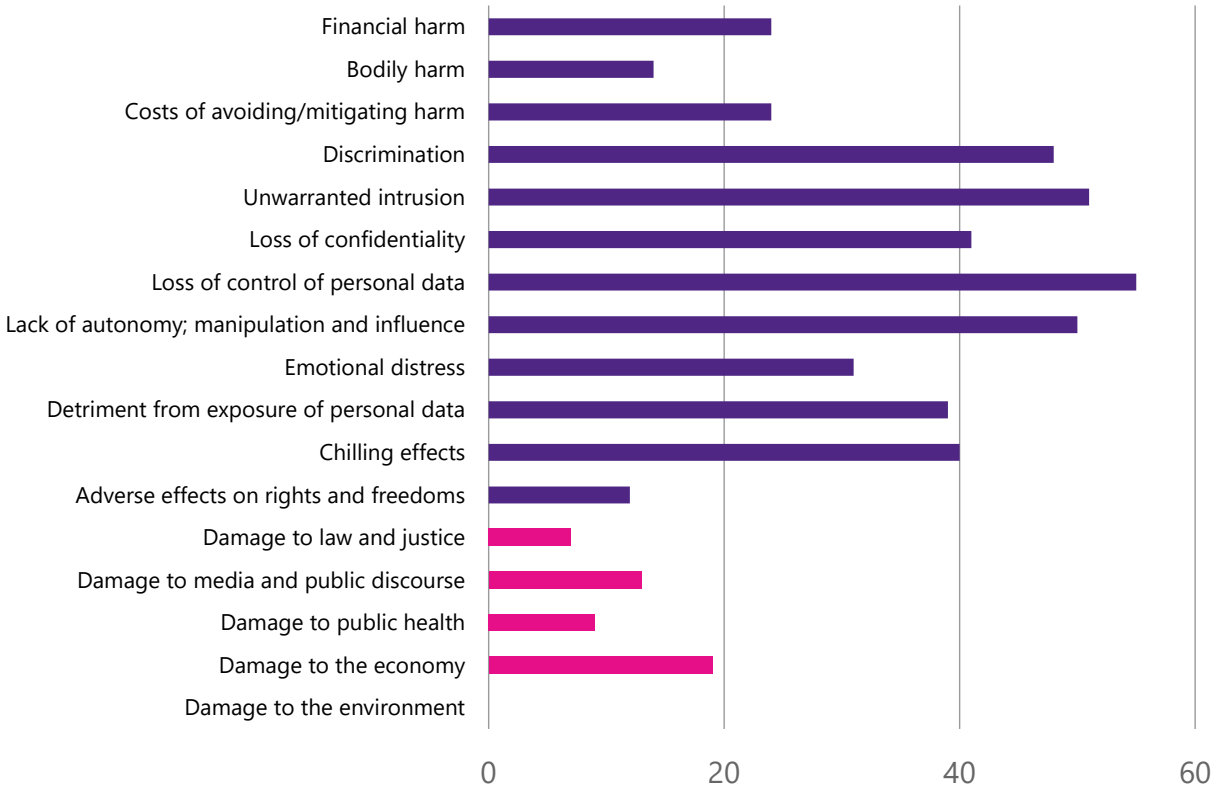


4.3 Mapping results to the ICO's data protection harm taxonomy

After the full text review, studies were assigned 'tags' corresponding to the ICO's taxonomy of data protection harms. The taxonomy consists of 12 categories of individual harms and 5 categories of societal harm. The taxonomy, along with relevant examples, is reproduced in Appendix B.

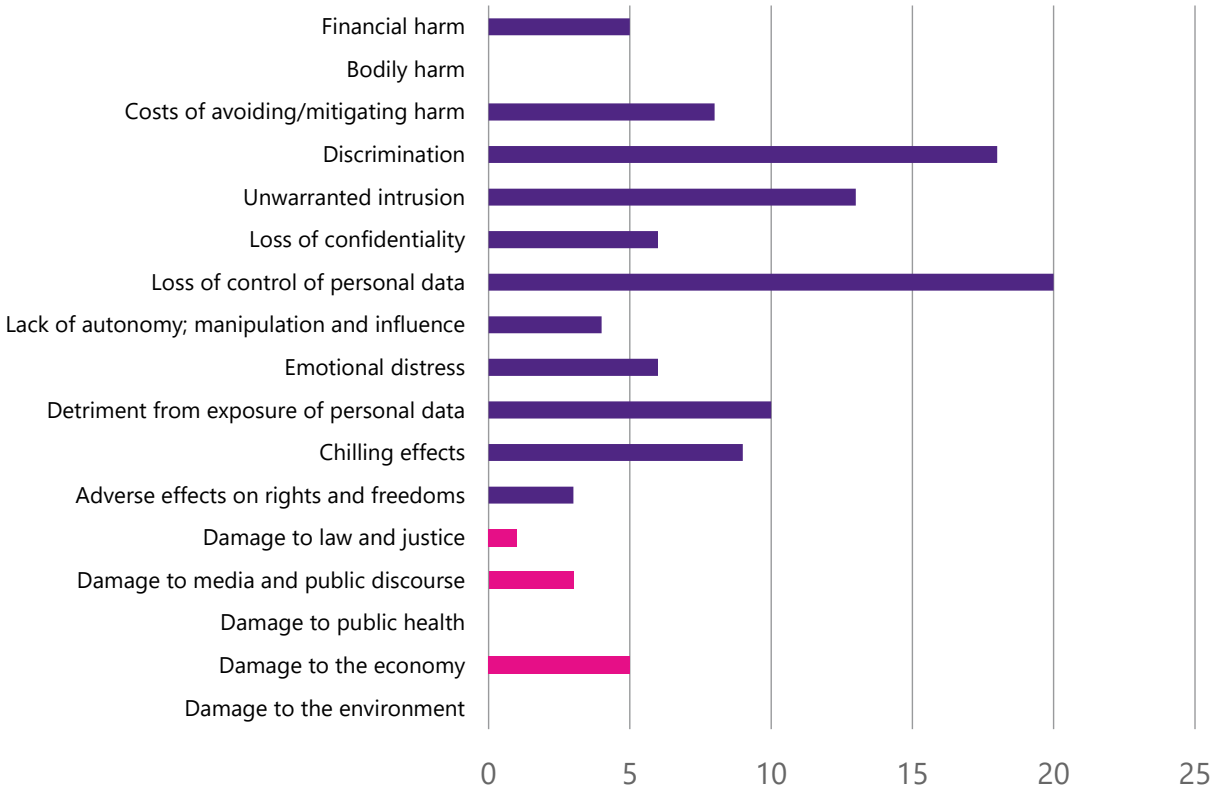
Studies were assigned tags if they examined, discussed or mentioned particular harms. Studies could be assigned any number of tags. To reduce the subjectivity in this process, the tags assigned were reviewed by a second reviewer. The total count of the tags assigned is shown in Figure 4.5.

Figure 4.5: Tag count



Studies were also assigned a 'primary' tag according to the particular harm on which they focused (Figure 4.6). Note that many studies discussed a number of different harms and assignation of a primary tag was not clear-cut. The primary tags assigned were reviewed by a second reviewer to reduce subjectivity.

Figure 4.6: Primary tag



4.4 Empirical evidence base

After assigning a tag to each of the studies, the records were further analysed to identify which data protection harms have a strong existing base of empirical evidence or that lack empirical evidence. The empirical evidence definition includes studies that conduct novel primary research i.e., experiments, focus groups, interviews, surveys, and mixed methods.[4]

The research methodology was compared against the data protection harm tags (Figure 4.7).

Figure 4.7: Empirical evidence by primary and secondary tag

Data protection harm tag	Primary tag – empirical studies	Secondary tag – empirical studies
Financial harm	2	9
Bodily harm	-	5
Costs of avoiding/mitigating harm	5	15
Discrimination	3	15
Unwarranted intrusion	7	22
Loss of confidentiality	1	13

[4] This definition of empirical evidence therefore excludes other research methods such as taxonomy, theoretical, evidence survey (i.e., review of theoretical and empirical literature) or case study methods.

Data protection harm tag	Primary tag – empirical studies	Secondary tag – empirical studies
Loss of control of personal data	13	30
Lack of autonomy; manipulation and influence	1	18
Emotional distress	2	7
Detriment from exposure of personal data	5	13
Chilling effects	7	24
Adverse effects on rights and freedoms	-	5
Damage to law and justice	-	-
Damage to media and public discourse	-	3
Damage to public health	-	3
Damage to the economy	-	8
Damage to the environment	-	9

Note that the count of empirical studies relevant to secondary tag is likely to be overrepresented. Several of the studies reviewed provide a broad discussion covering several data protection harms but the empirical evidence presented in the paper (e.g., the survey questions or focus group discussion) will be restricted to a subset of these harms.

The number of empirical studies varies significantly by tag. Some tags are relatively well explored in empirical studies, such as loss of personal data, unwarranted intrusion and chilling effects. In some areas, however, empirical evidence is relatively lacking. For example, no empirical studies assess damage to law and justice, and societal harms in general are not the primary focus of any empirical study.

These results also highlight potential evidence gaps for harms that are otherwise (theoretically) well explored in the literature. For example, discrimination and loss of confidentiality are key harms, widely discussed in the literature (as shown in Figure 4.5 and Figure 4.6) but are underrepresented in the empirical literature. It is therefore hard to judge data subjects' awareness and experience of these harms.

4.5 Data protection harms affecting particular groups

The records were then analysed to see if certain tags were more strongly associated with particular groups. The majority of studies are not specific to a particular group and focus a broad range of harms, with numerous secondary tags.

Several studies are specific to a situation affecting a certain group, such as criminals and ex-offenders or users of genetic testing. This, along with limited evidence for specific groups, makes it difficult to generalise or find trends that may affect these groups.

The table below highlights some high-level findings from the most studied groups.

Figure 4.8: Groups and types of harm

Group	Common themes
No specific group	The vast majority of studies explore the general impact of harms with no focus on a specific group or set of individuals. This set of studies broadly considers all harms. The most common primary tag for these studies are unwarranted intrusion, discrimination, and loss of control of personal data.
Adults	Adults are the main group studied after 'no specific group' category. This group is distinct, and generally specified to highlight that an empirical study surveyed or interviewed adults as part of primary data collection. The most common primary tags for these studies are loss of control of personal data, chilling effects, and costs of avoiding or mitigating harms.
Children	Children were the second most considered group. Unlike the 'adult' group, the majority of these studies are theoretical (not empirical) and focus on potential harms faced by children online or how children can be kept safe online. The most common primary tags for studies focusing on harm are loss of control of personal data, chilling effects, costs of avoiding or mitigating harms, and unwarranted intrusion.
Social media	Only six studies were dedicated to social media users. Although a limited evidence base, it is notable that the majority of these studies focus on harms arising from loss of control of personal data, detriment from exposure of personal data, and loss of confidentiality.
Groups facing discrimination	Discrimination is the most commonly assigned primary and secondary tag across all of the groups studied (i.e., present for the majority of groups). Discriminatory harm is particularly associated with ethnic minorities, users of genetic testing services, and individuals with disabilities.

5 Review findings

5.1 Review synthesis – primary question

Review existing evidence relevant to data protection harms, including evidence of awareness, risk and experience of individual and societal data protection harms.

In total 111 references were judged by the study team to be relevant to the review. The evidence found in our review come from a range of disciplines – including sociology, healthcare, marketing, information technology, economics, and law – indicating that a range of sectors are considering this issue. Grey literature is also a significant contributor to the knowledge base in this area.

Awareness of data protection harms

A number of studies and surveys explore individuals' awareness and concerns about data privacy. For instance:

- The ICO Annual Track surveys UK adults to assess their concerns and experience of online and data protection harm.[5] The latest survey of 2,102 adults found that 77% of respondents say protecting their personal information is essential;[6]
- A survey of 2,000 UK adults in 2020 found 77% of respondents are concerned about "companies selling on data about me";[7]
- A survey of 2,080 UK adult internet users in 2020, found that 45% were concerned about their personal info being stolen, up from 38% the year before;[8]
- In a survey of 2,026 UK adults, Benjamin (2020) found that 41% 'strongly agreed' that use of online personal data can be harmful to individuals;[9] and
- A survey of 27,607 EU citizens found four in ten (46%) Internet-using respondents are concerned about someone misusing their personal data, and 68% concerned that their online personal information is not kept secure by websites.[10]

In general, individuals express concern over the use of their personal data and say privacy is important to them. However, this is not always mirrored by their actions and behaviours – the so-called 'privacy paradox'.[11] This may be in part due to the transaction costs associated with fully evaluating the costs and benefits of signing up to an online service (i.e., this is time-consuming to do, so most users do not do it).

[5] ICO Annual Track research, 2018 to 2019: https://ico.org.uk/about-the-ico/research-and-reports/internet-users-experience-of-harm-online-ofcom-and-the-ico/
[6] ICO (2021), Information Rights Strategic Plan: Trust and Confidence. https://ico.org.uk/media/about-the-ico/documents/2620165/ico-trust-and-confidence-report-290621.pdf
[7] doteveryone (2020). People, Power and Technology: The 2020 Digital Attitudes Report
[8] Jigsaw Research (2020). Internet users' experience of potential online harms: summary of survey research. https://www.ofcom.org.uk/__data/assets/pdf_file/0024/196413/concerns-and-experiences-online-harms-2020-chart-pack.pdf [Jigsaw Research (2020)]
[9] Benjamin, G. (2020). Digital Society: Regulating privacy and content online. Solent University. https://pure.solent.ac.uk/en/publications/digital-society-regulating-privacy-and-content-online
[10] European Commission, Directorate-General for Migration and Home Affairs (2020). Europeans' attitudes towards cyber security, https://europa.eu/eurobarometer/surveys/detail/2249
[11] Refer to Acquisti et al (2016) for discussion of the privacy paradox.

There are also information asymmetries: some individuals may not be aware of the extent to which their personal information is collected or the uses it is put to. Which? (2021)[12] surveyed a panel of 4,014 UK consumers, and found that those who were informed about how Google and Facebook use their personal data had a higher willingness to pay (fee) to restrict the use of their personal data and a higher willingness to accept (i.e., monetary reward or compensation for personal data use) than uninformed consumers.

The privacy paradox has also been attributed to a growing 'fatalism'[13] or 'digital resignation'[14] among consumers. This stems from a view that individuals have little choice over what happens to their data, or little control over what happens to it once they start using an online service. Some individuals may view data processing as the 'price' they pay for free online products or services.[15]

Various studies have attempted to estimate how individuals value their privacy:

- Winegar and Sunstein (2019) find that the median consumer is willing to pay just $5 per month to maintain data privacy (along specified dimensions), but would demand $80 to allow access to personal data;

- In a study of Korean internet users, Lim et al (2017) estimate the compensation individuals would require for different types of personal information in a hypothetical data breach situation, finding that consumers generally placed high value on information that could cause immediate and actual damage if leaked, such as personal and payment information.

- Prince and Wallsten (2020) investigate how much compensation consumers would demand in order to share their data, and explore how this differs by country.[16] The authors find that people in Germany place a higher value on privacy compared to those in the US and Latin American countries.[17] The paper also finds that women value privacy more than men across different platforms, data types and countries, and that older people were more conservative (i.e. placed a higher value on privacy higher) than younger people.

While individuals may express general concern about data privacy, their awareness of specific harms resulting from a breach of their personal data appears to be more limited. There is some evidence for relatively high levels of concern about loss of financial data or online fraud.[18],[19] However, the CMA noted that "*consumers struggle to pinpoint specific examples of harms as a result of data processing or behaviourally based targeted advertising*".[20] Which? noted that "*When prompted to consider their non-financial data, most consumers simply cannot see how criminals could profit from this information*".[21]

[12] Which?, Accent and PJM economics (2021). Value of the Choice Requirement Remedy. Research Report, September 2021. https://www.which.co.uk/policy/digital/8107/value-of-the-choice-requirement-remedy
[13] Which? (2018) Control, Alt or Delete? The future of consumer data. https://www.which.co.uk/policy/digital/2659/control-alt-or-delete-the-future-of-consumer-data-main-report [Which? (2018a)]
[14] Helen Kennedy, Susan Oman, Mark Taylor, Jo Bates & Robin Steedman (2020). Public understanding and perceptions of data practices: a review of existing research. Living With Data, University of Sheffield. http://livingwithdata.org/current-research/publications
[15] CMA (2020). Online platforms and digital advertising market study. Final Report - Appendix L: summary of research on consumers' attitudes and behaviour. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
[16] Prince, Jeffrey, and Wallsten, Scott (2020). How Much is Privacy Worth Around the World and Across Platforms? Technology Policy Institute. https://techpolicyinstitute.org/wp-content/uploads/2020/02/Prince_Wallsten_How-Much-is-Privacy-Worth-Around-the-World-and-Across-Platforms.pdf
[17] The paper surveys individuals from Germany, the United States, Mexico, Brazil, Colombia and Argentina.
[18] Véliz, Carissa (2020). Data, Privacy and the Individual. Center for the Governance of Change. https://www.ie.edu/cgc/research/data-privacy-individual/
[19] Jigsaw Research (2020).
[20] Ibid.
[21] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use. https://www.which.co.uk/policy/digital/2707/control-alt-or-delete-consumer-research-on-attitudes-to-data-collection-and-use [Which? (2018b)]

Risk of data protection harms

To our knowledge, the risks of certain types of data protection harms occurring has not been explored in a systematic manner. This is likely to reflect the challenge in linking a specific data event (e.g. a data breach, or signing up to an online service) to a subsequent harm, which may occur months or years later.

There are various means by which personal data may be breached: for instance, via cyberattacks on firms or organisations,[22] via malware[23], or via inappropriate permissions.[24] However, the extent to which such breaches impact the risk of a given harm occurring is not well explored.

- Solove and Citron (2017) present the risk of harm as a harm itself. They argue that data-breach harms often result in victims experiencing anxiety about the increased risk of future harm, even where there is no proof that such harm has occurred. The authors also argue that even if *"seemingly innocuous data"* is compromised, it can lead to heightened risk of harm if aggregated with other data.[25]

- Livingstone, Stoilova and Nandagiri review evidence relating to online privacy risks affecting children, although it notes that the evidence on any negative consequences from breaches of children's privacy is scarce.[26] However, the review notes that children are perceived as more vulnerable than adults to privacy threats - due to their lack of digital skills or awareness of privacy risks – which would imply higher potential exposure to privacy harms.

- Bada and Nurse (2019) explore how members of the public perceive and engage with cyber risk, and how they are impacted during and after a cyber-attack.[27] The authors argue that cybersecurity-related decisions can induce anxiety and a sense of 'learned helplessness' wherein users may simply accept the possibility of being a victim.

- Milne et al (2017) attempt to map the type and severity of risk consumers perceive when sharing their personal data.[28] The authors use a survey methodology to ask individuals to rate the perceived risks (psychological, social, monetary and physical) around sharing different types of information. Passwords, medical data, insurance data, DNA and financial data were among the riskiest types of information.

Experience of data protection harms

Surveys generally ask about individuals' views, concerns, or perceptions of harms, rather than experiences. This may be because of challenges in finding people who have (knowingly) suffered data protection-related harms. However, some surveys have asked individuals about their experiences of harms:

- Ofcom (2017) found 4% of UK online adults reported financial/personal information being stolen and used online without their permission or knowledge.[29]

[22] Bada, Maria and Nurse, Jason R. C. (2019). The Social and Psychological Impact of Cyberattacks. In: Benson, Vladlena and McAlaney, John, eds. Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, London, pp. 73-92. ISBN 978-0-12-816203-3
[23] Urban, Tobias et al (2019). Analyzing Leakage of Personal Information by Malware. Journal of Computer Security, vol. 27, no. 4, pp. 459-481, 2019.
[24] ENISA (2018). Privacy and data protection in mobile applications: a study on the app development ecosystem and the technical implementation of GDPR. https://data.europa.eu/doi/10.2824/114584
[25] Solove, Daniel & Citron, Danielle. (2016). Risk and Anxiety: A Theory of Data Breach Harms. SSRN Electronic Journal. 96. 10.2139/ssrn.2885638.
[26] Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science.
[27] Bada, Maria and Nurse, Jason R. C. (2019). The Social and Psychological Impact of Cyberattacks. In: Benson, Vladlena and McAlaney, John, eds. Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, London, pp. 73-92. ISBN 978-0-12-816203-3
[28] Milne, George et al (2017). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing, Journal of Consumer Affairs, Wiley Blackwell, vol. 51(1), pages 133-161, March.
[29] Ofcom (2017). Adults' media use and attitudes report. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf

- Ablon et al (2016) ask if respondents have experienced a data breach, and asks them to place a notional monetary value on the cost to themselves of dealing with the breach.[30] 43% of respondents had received at least one notification of a data breach. Of these, 32% of respondents reported zero cost; but 6% reported a loss of over $10,000. The median loss among those who reported a loss was $500.

- Jigsaw Research (2020) found that despite high levels of concern, only 6% of adults have experienced personal information being stolen and non-consensual data use. However, 50% of those who had experienced theft of personal information found it "very annoying or upsetting".[31]

- A survey of 27,607 EU citizens found around one in ten know of someone who experienced online fraud (13%), hacking of an online social network or email account (12%), or who has been a victim of bank card or online banking fraud (10%).[32] 7% of respondents knew someone who has experienced identity theft.

There is, however, a data protection harm for which the prevalence can be assessed: chilling effects (a reduction in the use of services or activities due to an actual or perceived risk of potential harm). This is a topic covered in several recent studies:

- Cisco (2020) surveyed 2,600 adults in 12 countries about data privacy concerns. The survey found that 29% of respondents were "privacy actives" and had switched companies or providers over data protection concerns.[33]

- A survey of 1,000 US adults who had received a data breach notification found that 11 percent of respondents stopped interacting with the affected company, while a further 23% said they gave the company less business than before the breach. This effect did not differ significantly across age groups, however lower income customers were significantly more likely to stop interacting with the company.[34]

- In in-depth interviews with 10 US college student Facebook users Brown (2020) found that some had reduced their usage of the service after the Cambridge Analytica incident. While the interviewees reported concerns around use of Facebook, none had left Facebook permanently.[35]

5.2 Review synthesis – secondary questions

Identify areas where there are gaps in the evidence of data protection harms, and areas where the evidence is less robust.

Assess the evidence around the relative risk and severity of actual and perceived harms.

As part of our review we attempted to map the evidence we collated to the ICO's harms taxonomy (refer to Section 4.3). This highlighted some areas where there is comparatively less research. In particular:

- **Bodily harm**. No study in our review dealt primarily with physical harms related to data protection. While a number of studies explored such harm might arise,[36] they did not include estimates of

[30] Ablon, Lillian, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky (2016). Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information. RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1187.html [Ablon et al (2016)]
[31] Jigsaw Research (2020)
[32] European Commission, Directorate-General for Migration and Home Affairs (2020). Europeans' attitudes towards cyber security, https://data.europa.eu/doi/10.2837/6720239
[33] Cisco (2020), Consumer Privacy Survey. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf
[34] Ablon et al (2016).
[35] Brown Allison J. (2020). "Should I Stay or Should I Leave?": Exploring (Dis)continued Facebook Use After the Cambridge Analytica Scandal. Social Media + Society. January 2020.
[36] Lutz, Christoph and Ranzini, Giulia (2017). Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. The authors mention the prospect of physical harm arising as a result of sharing location data with other users.

prevalence. However, one study[37] did explore how connected devices interacted with domestic violence, and found that victimisation involving connected devices was likely to amplify the impact of domestic abuse.

- **Adverse effects on rights and freedoms**. While acknowledging that violation of privacy is itself an impingement of an individual's rights, few studies explored the knock-on effects on other rights and freedoms. One example of where this is explored is in relation to ex-offenders and discrimination. In this context, ex-offenders may be unable to exercise their right not to disclose a spent conviction to prospective employers, as employers may be able to find that information on the internet.[38]

- **Societal harms**. These harms are not well-explored in general. However:

  - some studies have explored harm to the economy due to competitive implications of data access. For example, Stucke and Ezrachi (2017)[39] discuss digital assistants and the potential harms that can arrive due to data collection and algorithms. The authors highlight that network effects and existing access to personal data (economies of scope from adjacent services) mean that leading digital assistants are likely to come from one of the big tech players. Not only does this disadvantage new entrants and may diminish innovation in the long-term, but personalised services may also diminish consumer welfare, privacy standards and democracy in favour of corporate interests; and;

  - some studies have explored the impact of voter microtargeting. For example, Magrani (2020) concludes that unauthorized personal data processing, along with misinformation and digital astro-turfing techniques, undermines voters' trust and the integrity of political processes., Rubinstein (2014) discusses the potential harms of voter microtargeting to the democratic process, which include 'political inequality' (wherein only a subset of 'strategic' voters receive any attention), manipulation or suppression of voter turnout, and 'superficial politics' (wherein voters receive individually calibrated but fragmented messaging which does not amount to a consistent whole).

As noted above, the risk of certain types of data protection harms occurring has not been explored in a systematic manner. As discussed, there may be a delay in a data breach event and the occurrence of a harm (although the original data breach event may cause risk and anxiety for the victim). This can make it difficult to assess the contributory factors to the risk of a harm occurring.

There are a number of surveys which ask respondents whether they have experienced data protection harms (refer to Section 5.1). Such surveys often ask about data protection harms in a general sense, rather than asking about specific harms. It is therefore challenging to assess the relative prevalence of many harms on the ICO taxonomy.

However, some surveys also ask about individuals' experience of scams/fraud, or other types of harms relating to data protection. For instance, Jigsaw Research surveyed 2,080 UK adults regarding their concerns and experiences of various types of online harms, and asked those who have experienced harm to rank the severity of the impact. While personal data theft was reported to happen with relatively low frequency, around 50% of those who had experienced it ranked it as "very annoying or upsetting".[40]

[37] Knittel, Megan and Shillair, Ruth (2020). Information Policy, Privacy Failings, and Steps Towards Empowerment in Cases of Technology-Facilitated Sexual Violence. TPRC48: The 48th Research Conference on Communication, Information and Internet Policy, Available at SSRN: https://ssrn.com/abstract=3748984 or http://dx.doi.org/10.2139/ssrn.3748984

[38] McIntyre, TJ; O'Donnell, Ian (2017). Criminals, Data Protection and the Right to a Second Chance. 58 Irish Jurist (ns) 27

[39] Maurice E Stucke and Ariel Ezrachi (2017). How Digital Assistants Can Harm Our Economy, Privacy, and Democracy. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2957960

[40] Jigsaw Research (2020)

In terms of severity of harms, a variety of studies discuss or explore the potential impacts and implications of a particular type of harm occurring (e.g. fraud or identity theft).[41] To our knowledge, no study has attempted to explicitly quantify the impact of a particular data protection harm. Again, this makes it challenging to assess the relative impact of different types of harm. However, some studies have asked users for their subjective assessment of the impact of a data protection harm on themselves.[42]

5.3 The ICO taxonomy and mapping process

Some findings were noted during the process of mapping the evidence uncovered to the ICO's harms taxonomy:

- Some of the harms categories are interrelated and were often used in tandem:
  - Loss of control of personal data and unwarranted intrusion;
  - Loss of confidentiality and detriment from exposure of personal data; and
  - Chilling effects and the cost of avoiding/mitigating harm.
- Some emerging research areas were found, including algorithmic discrimination, smart cities/IoT, direct-to-consumer genetic testing. Our review indicated that, of these areas, algorithmic discrimination and the potential adverse impact of AI technologies have received the most research attention. Studies come from a range of organisations (such as the CMA, Cisco and Data Justice Labs) and academic disciplines (including law, sciences, sociology). Smart cities/IoT and direct-to-consumer genetic testing are less explored, with studies limited to the relevant academic field; for example, genetics testing is explored in science/science ethics literature.
- "Discrimination" is one of the most commonly used tags. This is largely due to price discrimination, which is a relatively well-explored area in the economics literature. Discrimination against particular groups is less well-explored, although several studies examine the specific impact of data protection harms on low-income groups. As discussed in Section 4.5, these studies tend to focus how harms may affect a specific group in a particular context and tend not to examine how this experience varies from a counter-factual group (e.g., types and prevalence of harms affecting low-income or ethnic minority groups compared to other adults in general).
- Societal harms are not well understood in general. Economic harm is the most discussed in the theoretical literature, specifically with regards to data collection and how this may affect (digital) market concentration. Poor understanding of societal harms is further reflected by a general lack of empirical evidence exploring societal harms.

We also explored the interaction between the harms category a study had been tagged with (i.e. financial harm, physical harm) and whether the study undertook original primary research (e.g. surveys, focus groups). This provided several insights:

- While many studies discussed or considered the issue of discrimination, only around a third of studies with this tag undertook primary research.

[41] For example, Solove, Daniel & Citron, Danielle. (2016). Risk and Anxiety: A Theory of Data Breach Harms. SSRN Electronic Journal. 96. 10.2139/ssrn.2885638.
[42] E.g. Ablon et al (2016), Jigsaw Research (2020).

- Similarly, only around one quarter of studies which considered emotional distress undertook original primary research.

- 'Chilling effects' are relatively well explored by primary research – 60% of studies with this tag involved original primary research.

5.4 Other taxonomies

In conducting the review, we came across several studies which have developed taxonomies of data protection harms or related areas. These are discussed in summary below. A more detailed comparison of the taxonomies is provided in Appendix C.

- Agrafiotis et al (2016) develop a taxonomy of cyber harms, differentiating between direct (immediate) and indirect (secondary or long-term) harms (refer to Figure 5.1). Note that this taxonomy does not exclusively concern data protection harms.

- Agrafiotis et al (2018) develop a taxonomy of cyber harms for cyberattacks on organisations which comprises five broad themes: physical or digital harm; economic harm; psychological harm; reputational harm; and social and societal harm.

- Calo (2011) proposes a classification of privacy harm into two categories. Objective harms involve unanticipated or coerced use of information concerning a person against that person (e.g. identity theft). Subjective harms include unwelcome mental states—anxiety, embarrassment, fear—that stem from the belief that one is being watched or monitored.

- ENISA (2013) develops a methodology for the assessment of the severity of personal data breaches. This discusses the different types of personal information which may be compromised and attaches a score to them.

- Slaughter (2021) outlines the taxonomy of harms caused by algorithmic decision-making. This includes flaws in algorithm design that frequently contribute to discriminatory or otherwise problematic outcomes in algorithmic decision-making. It also considers societal-level harms: harms to civil justice, harms to economic justice and surveillance.

- Citron and Solove (2022, forthcoming) construct a typology for harms resulting from privacy violations. This groups harms into seven basic types: physical, economic, reputational, psychological, autonomy harms, discrimination harms, and relationship harms.

- Milne et al (2017) develop an 'information sensitivity typology' to map the perceived risk in personal data sharing. The typology consists of four broad risk categories: monetary, social, physical and psychological.

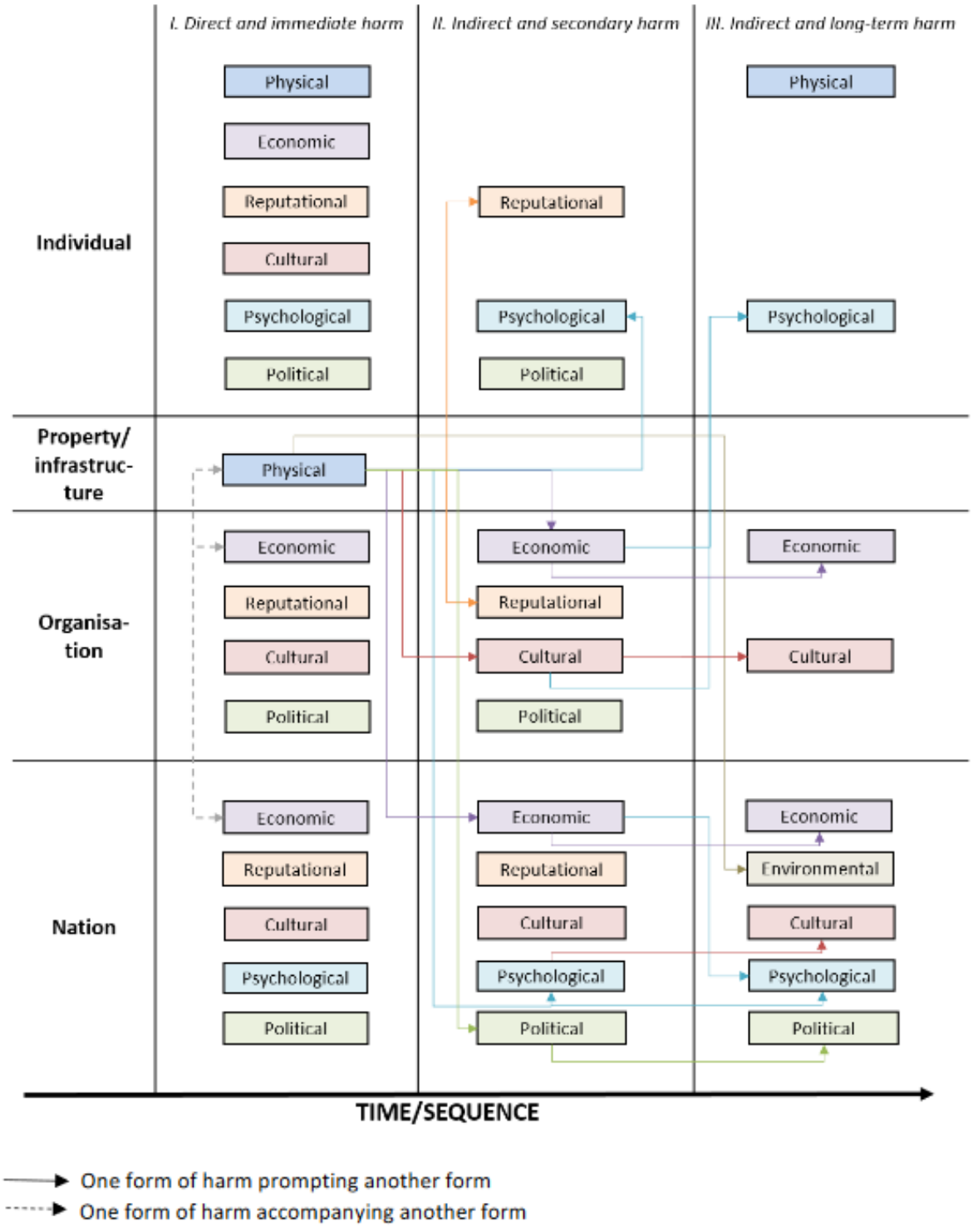
- Kröger et al (2021, preprint) propose eleven categories of personal data misuse, and provide 2-3 illustrative examples for each. These categories (and examples) include: consuming data for personal gratification (e.g., ridicule and voyeurism), generating coercive incentives (e.g., threats of physical violence, personalised rewards, personalised sanctions, blackmail), compliance monitoring (e.g., political oppression, domestic abuse, workplace surveillance), discrediting the data subject (e.g., publication of sexual imagery, political discrediting tactics, legal evidence), assessment and discrimination (e.g., identification of political opponents, discriminatory hiring practices, discriminatory pricing or provision of services), identification of personal weak spots (e.g., torture, bullying, legal vulnerabilities), personalised persuasion (e.g., commercial advertising, political targeting, social engineering attacks or "phishing"),

contacting the data subject (e.g., fraudulent messages and unsolicited advertising, threats and letter bombs, online sexual predation), locating and physically accessing the data subject (e.g., sex crimes, organised crime, persecution based on race, religion or political beliefs), accessing protected domains or assets (e.g. social media burglary, identity theft), and reacting strategically to actions/plans of data subject (e.g., stifling political resistance, predictive policing, forestalling legal action).

- Data Action (2022a, draft) outline an online harms taxonomy that is broadly grouped into five areas: disinformation & misinformation, hate speech and incitement, online harassment & abuse, online censorship, and infringements of privacy. The taxonomy groups each of the five harm areas into impact on democracy and impact on human rights.

- Data Action (2022b, draft) describe a tech accountability policy taxonomy. These cover six key areas: transparency, (political) advertising, algorithms & content curation, community standards/content moderation/company enforcement, liability & enforcement, and privacy & data protection. This outlines, and provides examples of, types of government and company policy that have "the greatest potential to have a positive impact on [three specific areas] democracy, human rights and online harms, and that deal with the systematic problems with the ad-tech model".

Figure 5.1: Layers of cyber harm (Agrafiotis et al)



Source: reproduced from Agrafiotis et al (2016).

5.5 Research by authorities in other jurisdictions

As part of the study, we also examined the relevant data authorities in some major countries: France, Germany, Italy, Spain, and the United States. We reviewed the websites of the relevant authorities (and related organisations) in each country for research or evidence of data protection harms in that jurisdiction.

The ICO's work on the issue of data protection harms appears relatively advanced compared to other regulators – for example, in our review, we did not come across an attempt to develop a taxonomy of data harms.

- In **France**, the data protection authority Commission Nationale Informatique et Libertés (CNIL) publishes some tools to help users with data protection concerns. The starting point for research appears to be not the category of data harms but by category of abuse (e-commerce, nuisance calls, online harassment). The number of data violations is reported yearly (2000 in 2018)[43] – but this is likely an underestimate.

- **Germany** is relatively advanced in terms of action on online harms in general. The NetzDG ("Act to Improve Enforcement of the Law in Social Networks") came into force in 2017, and was last amended April 2021. Its aim is to tackle hate and other harmful content on social networks, but not to specifically address data issues. The data protection regulator, BfDI, allows users to complain and publishes some limited information, but no research. Its focus appears to be on ensuring compliance with GDPR.

- In **Italy**, the data protection authority (Garante per la protezione dei dati personali) publishes an annual report. We could not find any research on data protection harms.

- In **Spain**, the data protection authority (AGPD) publishes a number of guides and tools for users and data processors, including how to carry out data protection impact assessments.[44] We could not find any research on data protection harms.

- The **United States** has a "patchwork" of federal data protection laws rather than a single comprehensive data protection law. Relevant bodies at the federal level include the Federal Trade Commission (FTC) and the Privacy Office. Neither appears to have published research on the issue of data protection harms. However, some relevant research is published by other entities, such as the Pew Research Centre.

  At the state level, some states have passed data privacy laws (California, Colorado and Virginia) and bills are in active discussion in some other states.[45] In most states, this means companies can use, share, or sell any user data they collect without notifying the user.[46]

  In 2018, California signed into law the California Consumer Privacy Act (CCPA), which follows in the footsteps of GDPR. Among other rights, it provides users the right to opt out of sharing personal data.[47] In November 2020, California voters approved Proposition 24, the California Privacy Rights Act of 2020 (CPRA). The CPRA added new privacy protections to the CCPA and created the California Privacy Protection Agency.[48] This does not appear to have published any research as yet.

[43] https://e-enfance.org/informer/violation-des-donnees-personnelles/
[44] For example, 'Risk management and impact assessment in personal data processing' (in Spanish), published 29 June 2021. Refer to: https://www.aepd.es/es/guias-y-herramientas/guias
[45] Refer to https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
[46] https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/
[47] https://oag.ca.gov/privacy/ccpa
[48] https://cppa.ca.gov/

6 Recommendations

As part of our review, we found several other attempts to develop taxonomies for data protection harms or harms in closely related areas. We have carried out additional analysis of these taxonomies and compared them to the ICO's own harm taxonomy (refer to Appendix C).

In general the ICO's data protection harms taxonomy is comprehensive: few harms appear on other taxonomies but not on the ICO's taxonomy. The key examples here are relationship harms and cultural harms, though these potentially overlap with other harms on the ICO's taxonomy.

The comparison exercise also suggests that the ICO is relatively advanced in its thinking on societal-level harms, which are not well-represented in other taxonomies. For instance, the ICO has distinguished between individual-level financial harms and economywide harms (which tend to be grouped together in other taxonomies).

However, there may still be opportunities to refine the ICO's taxonomy. We suggest the ICO:

- considers separating price discrimination and discrimination against protected characteristics into two distinct harms. These two harms manifest for different reasons and are likely to have different impacts;
- considers relabelling 'emotional distress' as 'psychological harm'. This brings the terminology closer to that employed in other taxonomies and studies, and is also broader;
- considers a separate societal harm category for harms to the political/democratic process, or explicitly refer to the democratic process within '*Damage to media, information and public discourse*'.

There are also harms within the ICO taxonomy which are interrelated and were often used in tandem during the tagging process of this review. This may present opportunities to refine the taxonomy.

- '*Loss of confidentiality*' is related to '*Detriment from exposure of personal data*'.
- *'Loss of control of personal data'* is related to *'Lack of autonomy; manipulation and influence'* and *'Loss of confidentiality'*.
- *'Costs of avoiding/mitigating harm'* and *'Chilling effects'* are related, insofar that discontinuing the use of a service over privacy concerns is a type of cost of avoiding harm.

Our review also uncovered a number of areas where there is relatively less evidence (or where the available evidence is largely theoretical). This may present opportunities for further research.

- As noted above, the ICO is a leader in conceptualising societal-level harms. These harms are not well explored in the existing literature. We suggest the ICO continues its work in developing the theoretical basis for these harms. Once the theoretical basis is developed the ICO should explore opportunities for empirical research in this area.
- There are some gaps in the empirical evidence, particularly around the impact of psychological harms and the prevalence of certain types of harm (e.g. bodily harm).
- Studies which explore the prevalence or impact of certain harms to particular groups (e.g. children) often do not set up a 'baseline' – that is, how prevalent or impactful that harm is in the general population. This makes it challenging to assess the relative impact of harms across groups.

Some evidence in the review supports the idea of a mismatch between individuals' reported concerns about use of their personal data and their observed actions and behaviours (for example, signing up to a service without reading the terms of service). This is sometimes referred the 'privacy paradox'.

A number of explanations have been advanced for this mismatch, including asymmetric information, a lack of understanding of how personal data is used (or can be harmful), a lack of alternative services, choice architecture (or the way privacy options are framed), or user apathy and 'digital resignation'. The evidence also suggests that the more individuals are informed about how their data are used, the greater reward they demand to share that data.

This may present a fruitful area for further research into the drivers of individuals' behaviour and their motivations. For example: do individuals sign up to digital services because they do not understand which data will be collected and how they will be used? Or are they cognisant of these risks, but sign up anyway because there are no alternative options? Understanding these drivers, and how they differ across groups, will help deepen the understanding of how individuals and society can become exposed to data protection harms.

Appendix A Search results

This appendix presents the number of hits for each combination of search keywords across the various search sources. For further details on the search strategy, refer to Section 3.

Figure A.1: EBSCO results

Title contains	AND text contains:	AND text contains:	Number of hits
"data protection" OR "data security" OR "personal data" OR "personal information" OR (privacy AND data OR harm)	harm		663
	harm	Risk	434
	harm	Awareness	145
	harm	Experience	202
	harm	Impact	295
	harm	Abuse	130
	harm	Individual	466
	harm	Societal	74
	harm	Financial	348
	harm	Emotional	52
	harm	Economic	310
	harm	Environmental	63
	harm	"Loss of control"	24
	harm	Rights	474
	harm	Discrimination	97

Note: Searches carried out 01/12/2021. Results reflect studies from 2010 onward.

Figure A.2: JSTOR results

Title contains	AND text contains:	AND text contains:	Number of hits
"data protection" OR "data security" OR "personal data" OR "personal information" OR (privacy AND data OR harm)	harm		193
	harm	Risk	121
	harm	Awareness	42
	harm	Experience	63
	harm	Impact	89
	harm	Abuse	39
	harm	Individual	176
	harm	Societal	108
	harm	Financial	124
	harm	Emotional	22
	harm	Economic	103
	harm	Environmental	77
	harm	"Loss of control"	7
	harm	Rights	165
	harm	Discrimination	46

Note: Searches carried out 26/11/2021. Results reflect studies from 2010 onward.

Figure A.3: SSRN results

Text contains	Number of hits
Data privacy harm*	211
Data protection harm*	191

Note: Searches carried out 02/12/2021.

Figure A.4: Google search results

Text contains	AND text contains:	AND text contains:	Number of hits (approximate)
"data protection" OR "data security" OR "personal data" OR "personal information" OR (privacy AND data OR harm)	harm		65m
	harm	Risk	59m
	harm	Awareness	39m
	harm	Experience	57m
	harm	Impact	16m
	harm	Abuse	316m
	harm	Individual	72m
	harm	Societal	61m
	harm	Financial	18m
	harm	Emotional	22m
	harm	Economic	36m
	harm	Environmental	28m
	harm	"Loss of control"	6m
	harm	Rights	21m
	harm	Discrimination	8m

Note: Searches carried out 03/12/2021.

Figure A.5: Google scholar search results

Text contains	AND text contains:	AND text contains:	Number of hits (approximate)
"data protection" OR "data security" OR "personal data" OR "personal information" OR (privacy AND data OR harm)	harm		1,230,000
	harm	Risk	576,000
	harm	Awareness	188,000
	harm	Experience	600,000
	harm	Impact	727,000
	harm	Abuse	164,000
	harm	Individual	813,000
	harm	Societal	66,000
	harm	Financial	271,000
	harm	Emotional	132,000
	harm	Economic	336,000
	harm	Environmental	238,000
	harm	"Loss of control"	18,000
	harm	Rights	909,000
	harm	Discrimination	55,000

Note: Searches carried out 02/12/2021.

Appendix B The ICO harms taxonomy

Figure B.1: ICO data protection harms taxonomy - individual harms

Category	Description	Examples
Financial harm	Negligently, knowingly, or purposefully paving the way for financial losses to occur	Fraud; Impact on credit rating; Extortion; User Damages
Bodily harm	Negligently, knowingly, or purposefully paving the way for physical injury to occur	Suicide or other self-harm; Assault
Costs of avoiding/mitigating harm	The cost incurred in the avoidance or mitigation of harms or vulnerabilities related to data privacy	Time spent avoiding harm/risk of harm; Security costs
Discrimination	Harms arising from discrimination or bias (either conscious or unconscious)	Entrenched bias in automated decisions; Price discrimination
Unwarranted intrusion	Unwanted communications or intrusions that disturb tranquillity, interrupt activities, sap time or increase the risk of other harms occurring	Targeted advertising; Nuisance calls or spam; Unwarranted surveillance
Loss of confidentiality	Loss of confidentiality with the potential to lead to other harms or an increased risk of harm	Reversed pseudonymisation; Breach leading to fraud or spam; Damage to personal or professional relationships
Loss of control of personal data	Harms from thwarted expectations, through misuse, repurposing, unwanted retention or continued use and sharing of personal data, including a lack of commitment to the accuracy of data	Unwarranted surveillance; Failure to maintain data quality; Injury to peace of mind & ability to manage risk; Restrictions on ability to access/review use of personal data; Incompatible repurposing leading to distress
Lack of autonomy; manipulation and influence	Restriction, coercion, or manipulation of people's choices or their ability to make an informed choice	Unwarranted nudging; Power and information asymmetry
Emotional distress	Negligently, knowingly, or purposefully paving the way for emotional distress to occur	Detriment to mental health; Loss of sense or control of identity; Distressed relationships; Loss of confidence
Detriment from exposure of personal data	Detriment such as relationship breakdown, reputational damage or harassment/bullying brought on through exposure of personal data	Relationship breakdown; Reputational loss/loss of standing; Harassment/bullying; Stigmatisation
Chilling effects	Reduce use of services or activities due to an actual or perceived risk of potential harm	Reduced activities requiring good credit rating; Fear of sharing data due to perceived risk
Adverse effects on rights and freedoms	Negative impacts on rights and freedoms in and of themselves	Restrictions to data privacy rights; Restrictions to freedom of assembly; Chilling effects on freedom of expression

Source: ICO

Figure B.2: ICO data protection harms taxonomy - societal harms

Category	Description	Examples
Damage to law and justice	Restrictions on or subversion of legislative intent, or legal or judicial process	Creating a route for widescale subversion of a law; Chilling effects on victims or witnesses
Damage to media, information and public discourse	Negative impacts on media, information and public discourse at a societal level	Mistrust in handling of electoral role influencing elections or voter turnout; Widespread mistrust leading to chilling effects on freedom of expression
Damage to public health	Harms resulting in adverse health outcomes for society	Mistrust in handling of health data leading to chilling effects on health service use
Damage to the economy	Negative impacts on the economy that are significant at the local, regional, or national level, or for a specific sector	Loss of trust from widespread privacy abuses leading to chilling effects on major services; Misuse of personal data leading to unfair competitive advantage
Damage to the environment	Negative impacts on the environment either directly or indirectly resulting from misuse of data or mitigation of associated risk.	High energy use associated with data mining, storage and sharing; Loss of ecological diversity and/or green space due to land use for server farms

Appendix C Comparison of taxonomies

We have attempted to contrast the ICO's harms taxonomy with selected other taxonomies found in the review (Appendix C, Figure C.1 and Figure C.2). Note that some taxonomies [Calo (2011), ENISA (2013)] were not mapped as they are not directly comparable to ICO's.

The comparison of the taxonomies reveals a broad range of both harms and the terms used to describe them. However, these the terms tend to be very context specific – e.g., taxonomies for cyber harms will include different harms (and terms) to algorithmic harms or data protection harms.

Most taxonomies classify the types of harms according to the impact. A minority classify ways in which harms may occur (Slaughter, 2021; Kröger et al, 2021). As a result, the same harms (impacts) are sometimes listed in multiple categories of the taxonomy.

Some key differences between the ICO taxonomy and the other taxonomies are listed below.

- 'Financial harm' is widely referred to and/or classified as part of 'economic harm' (i.e., loss to individuals, organisations and wider economy).
- 'Emotional distress' is commonly referred to as 'Psychological harm' in other taxonomies. Citron and Solove (2022) differentiate between two types of 'Psychological harm': emotional distress (painful or unpleasant feelings) and disturbance (disruption to tranquillity and peace of mind).
- Certain harms identified by the ICO are not expressed in other taxonomies. These include 'Costs of mitigating/avoiding harm' and 'Damage to environment'. In addition, 'chilling effects' and 'adverse impact on freedoms and rights' are generally not well explored.
- The ICO taxonomy is notable for its classification of individual harms and societal harms. Other taxonomies tend to focus on individuals and/or organisations rather that wider societal impacts. Data Action's (2022a, 2022b) taxonomies are an exception as they are designed to focus on the impact on human rights and on democracy, at both individual and societal level.

Figure C.1: Taxonomy comparison (1 of 2)

Organisation /author	ICO taxonomy	Agrafiotis et al (2016)	Agrafiotis et al (2018)	Slaughter (2021)	Citron and Solove (2022, forthcoming)
Application areas	Data protection harms	Cyber harms	Cyber harms for cyber-attacks on organisations	Algorithmic decision-making	Harms resulting from privacy violations
Subject	Individuals and society (not businesses and government actors)	Individuals, organisations, property/infrastructure, nations (government and citizens)	Organisations, stakeholders (e.g., customers, service users)	Individuals (consumers and citizens)	Primarily individuals, secondary impact on organisations
Type of harms – mapped to the ICO's taxonomy	**INDIVIDUAL HARMS**				
	Financial harm	Economic harm (financial loss to individual or organisations)	Economic harm (i.e., harm that relates to negative financial or economic consequences)		Economic harms (primarily financial loss and damage to individual)
	Bodily harm	Physical harm (bodily injury, property damage, etc)	Physical/Digital harm (i.e., harm describing a physical or digital negative effect on someone or something)	Surveillance capital (can undermine consumers' mental health)	
	Costs of avoiding/mitigating harm				
	Discrimination			Proxy discrimination Faulty conclusions Failure to test	Discrimination harms
	Unwarranted intrusion			Surveillance capital (e.g., tracking and data collection, targeted advertising) Faulty inputs (e.g., inferred characteristics)	Autonomy harms (failure to inform, thwarted expectations)
	Loss of confidentiality				Autonomy harms (failure to inform, lack of control)

Organisation /author	ICO taxonomy	Agrafiotis et al (2016)	Agrafiotis et al (2018)	Slaughter (2021)	Citron and Solove (2022, forthcoming)
	Loss of control of personal data		Physical/Digital harm (such as exposed/leaked data, identity theft)	Faulty inputs Faulty conclusions	Autonomy harms (failure to inform, thwarted expectations, lack of control)
	Lack of autonomy; manipulation and influence			Faulty conclusions	Autonomy harms (coercion, manipulation)
	Emotional distress (embarrassment, anxiety, fear)	Psychological/emotional (depression, panic/stress, anxiety, self-harm, virtual harm, etc)	Psychological harm (i.e., harm that focuses on an individual and their mental well-being and psyche)	Surveillance capital (can undermine consumers' mental health)	Psychological harms (emotional distress, disturbance)
	Detriment from exposure of personal data		Reputational harm (i.e., harm pertaining to the general opinion held about an entity, such as reduced credit score) Physical/Digital harm (including identify theft)		Reputational harms
	Chilling effects				Autonomy harms (chilling effects)
	Adverse effects on rights and freedoms				
	SOCIETAL HARMS				
	Damage to law and justice	Political/governmental (disruption to electoral system, loss of citizen trust in government, reduction in power projection)			
	Damage to media, information, and public discourse	Political/governmental (as above)	Reputational harm (i.e., harm pertaining to the general opinion held about an entity)	Surveillance capital (business model promoted misinformation and disinformation)	
	Damage to public health				

Organisation /author	ICO taxonomy	Agrafiotis et al (2016)	Agrafiotis et al (2018)	Slaughter (2021)	Citron and Solove (2022, forthcoming)
	Damage to the economy	Economic harm (such as financial loss, loss of shareholder value, job loss, market degradation, etc)	Economic harm (i.e., harm that relates to negative financial or economic consequences, such as reduced providers or regulatory fines)	Threats to Competition Surveillance capital (can reduce or eliminate consumer choice)	Economic harms (primarily financial loss and damage to individual)
	Damage to the environment				
Other types of harm		*Reputational* (reduced consumer base, deteriorated international relations, etc) *Cultural* (loss of communication means, loss of cultural property, harms to social values, etc)	*Social and Societal harm* – generalised category (i.e., a capture of harms that may result in a social context or society more broadly)	Slaughter broadly groups harms into *Algorithmic Design Flaws and Resulting Harms* (Faulty inputs, Faulty conclusions, Failure to test) and *How Sophisticated Algorithms Exacerbate Systemic Harms* (Proxy discrimination, Surveillance capital, Threats to Competition).	Citron and Solove identify seven categories of harm. Including an additional category, *Relationship harms,* which involve damage caused to important relationships that are important to one's health, well-being, life activities affecting personal and professional relationships and relationships with organisations. Several distinct sub-harms are identified for *Psychological harms* and *Autonomy harms*.

Figure C.2: Taxonomy comparison (2 of 2)

Organisation /author	ICO taxonomy	Milne et al (2017)	Kröger et al (2021, preprint)	Data Action (2022a, draft)	Data Action (2022b, draft)
Application areas	Data protection harms	Personal data sharing & perceived risk	Data misuse – taxonomy focuses types of misuse, rather than harm generated	Online harms	Tech accountability policy (to limit impact of online harm) – *Privacy & Data Protection* subgroup
Subject	Individuals and society (not businesses and government actors)	Individuals (consumers)	Individual (consumer, citizen)	Individual – impact on democracy and human rights	Organisations, including companies and government
Type of harms – mapped to the ICO's taxonomy	**INDIVIDUAL HARMS**				
	Financial harm	Monetary risk (i.e., risk associated with potential financial loss such as fraud, identity theft, hacking financial accounts)	Identification of personal weak spots (screening for (financial) vulnerabilities)		
	Bodily harm	Physical risk (i.e., risk associated with potential financial loss such as harassment, stalking, physical threats)	Location and physically accessing data subject (tracking and direct contact e.g., sex crimes) Generating coercive incentives		
	Costs of avoiding/mitigating harm				
	Discrimination	Social risk (including risk associated with perceptions of others)	Assessment and Discrimination (e.g., discriminatory hiring, price discrimination)	Hate speech & incitement, Online censorship (targeting minority groups)	Hate speech & incitement Online harassment & abuse Non-discrimination, protections & security Freedom of expression/belief/ association

Organisation /author	ICO taxonomy	Milne et al (2017)	Kröger et al (2021, preprint)	Data Action (2022a, draft)	Data Action (2022b, draft)
	Unwarranted intrusion		Compliance monitoring (ensure people adhere to certain rules e.g., domestic abuse, workplace surveillance) Personalised persuasion (e.g., targeted advertising, political campaigns, phishing) Contacting data subject (unsolicited contact e.g., fraudulent messages, online sexual predation)	Online harassment & abuse Infringements of privacy (surveillance)	Disinformation & misinformation Hate speech & incitement Online harassment & abuse Online censorship
	Loss of confidentiality			Infringements of privacy (data breaches etc)	Online harassment & abuse
	Loss of control of personal data		Accessing protected domains or assets (e.g., social media burglary. identify theft) Identification of personal weak spots (screening for vulnerabilities e.g., bullying, legal vulnerabilities)	Infringements of privacy	
	Lack of autonomy; manipulation and influence		Generating coercive incentives (to affect behaviour (e.g., black mail) Compliance monitoring (e.g., workplace surveillance) Personalised persuasion (e.g., targeted advertising, phishing) Reacting strategically to actions/plans (e.g., stifling political resistance, predictive policing)	Online censorship	Disinformation & misinformation Online censorship

Organisation /author	ICO taxonomy	Milne et al (2017)	Kröger et al (2021, preprint)	Data Action (2022a, draft)	Data Action (2022b, draft)
	Emotional distress (embarrassment, anxiety, fear)	Psychological risk (i.e., risk associated with potential negative emotions such as anxiety, distress, and/or conflict with self-image) Social risk (including threat to self-esteem)	Consuming data for personal gratification without data subject's consent (e.g., ridicule, voyeurism)	Hate speech & incitement (impact on mental health of those targeted) Online harassment & abuse	Hate speech & incitement Online harassment & abuse
	Detriment from exposure of personal data	Social risk (including threat to reputation)	Discrediting (ways to cause legal and/or reputation harm e.g., publication of sexual images, political discrediting) Identification of personal weak spots (screening for vulnerabilities (physical, psychological, financial) e.g., bullying, torture, legal vulnerabilities)	Disinformation & misinformation, Online harassment & abuse (privacy and defamation)	As above.
	Chilling effects			Disinformation & misinformation (chilling effects on freedom of expression, belief – "censorship through noise") Hate speech & incitement Online harassment & abuse (withdrawing from public debate) Infringements of privacy (chilling effect due to data collection)	Chilling effects due to experience of other harms noted e.g., democratic harms leads to lack of engagement
	Adverse effects on rights and freedoms		Identification of personal weak spots (screening for vulnerabilities (physical, psychological, financial) e.g., legal vulnerabilities)	Online harassment & abuse Online censorship (limiting access to information or expression) Infringements of privacy (invasive data collection)	Freedom of information Online censorship Non-discrimination, protections & security Freedom of expression/belief/ association

Organisation /author	ICO taxonomy	Milne et al (2017)	Kröger et al (2021, preprint)	Data Action (2022a, draft)	Data Action (2022b, draft)
	SOCIETAL HARMS				
	Damage to law and justice		Discrediting (legal and/or reputational harm) Reacting strategically to actions/plans (e.g., predictive policing, forestalling legal action)		Rule of law/separation of powers/independent judiciary, Accountability in public admin, Free & fair elections, pluralistic politics
	Damage to media, information, and public discourse		Compliance monitoring (e.g., political oppression) Assessment and Discrimination (e.g., identification of political opponents)	Disinformation & misinformation (e.g. undermining elections) Abuse, hate speech and incitement (impact on democracy and pluralism), Online censorship	Plural and free media Disinformation & misinformation Hate speech & incitement Online harassment & abuse Online censorship
	Damage to public health			Disinformation & misinformation (undermining trust in public health professionals and treatments) Abuse, hate speech & incitement (impact on mental health)	
	Damage to the economy				
	Damage to the environment				
Other types of harm, comments		Social risk category covers several areas of the ICO's taxonomy. It is broadly defined as: *"Reputation, ratings, credibility in online communities and social networks, information in user profiles, longevity of stored information online, and lack of control over postings."*	Taxonomy focuses or motivations for misuse that cause harms, rather than categorising harms.	Note, list above is not complete taxonomy but highlights main commonalities and differences to ICO taxonomy. Common harms (outcomes) noted under different ways harms can arise	This taxonomy comprises six policy areas: *Transparency,* *(Political) Advertising;* *Algorithms and Content Curation;* *Community standards, content moderation and enforcement;* *Liability and Enforcement;* and *Privacy and Data Protection* (main focus of entries above)