2 March 2020

The Information Accountability Foundation ("IAF") appreciates the opportunity to comment on the **Draft Direct Marketing Code of Practice** ("Draft Code") produced by the Information Commissioner's Office ("ICO") and congratulates the ICO for a very thorough code that covers direct marketing from collection and processing of personal data to communications. Direct marketing as conducted today raises issues. The level of observation has accelerated over the past 25 years, and this increase has impacted direct marketing. With hundreds of parties placing third party cookies, accountability is, at best, inconsistent and, at worst, nonexistent. Furthermore, there are cases where persuasive communication has been used to manipulate people in a manner that violates the fundamental rights of individuals. Given these developments and the complexity of the number of participants there are in today's data ecosystem, it is clear that guidance related to marketing is warranted, and the IAF appreciates the challenges in drafting a code of practice in this arena. However, the IAF team has concerns that it believes the ICO should consider.

The IAF is a non-profit global information policy think tank that successfully works with regulatory authorities, policymakers, business leaders, civil society and other key stakeholders around the world to help frame and advance data protection law and practice through accountability-based information governance. Our goal, through active consultations and research, is to achieve effective information governance systems to facilitate information-driven innovation while protecting individuals' rights to fair processing and autonomy. The IAF's roots lie in its incorporation of the Global Accountability Dialog that helped define 21st century understanding of the accountability principle as applied to data protection. That work was also built on the key concept that "knowledge discovery" using data, which is similar to scientific research, usually does not directly impact people, and therefore, in most situations, does not create a significant effect on individuals. The following comments reflect the views of [redacted] and do not necessarily reflect the views of the IAF corporate and policy boards or funders.

Overview: Risk and Harm

Underlying the IAF concerns are the differences between privacy and data protection as fundamental rights. The right to privacy relates to individual autonomy and family life while the right to data protection relates to the risk to people arising out of the processing of data pertaining to them. The right of individuals to control their data, as a privacy right, is always important, but it is particularly so in instances where individuals should have to ability to protect themselves and their families and to form and socialize new ideas with a small circle of chosen friends. Consent as a governance mechanism works most effectively in situations where individuals knowingly provide data. Increasingly, data have their origin either in individuals' interaction with the world (observed) or in the insights that come from processing data (inferred). The legal basis for that processing increasingly is legitimate interests or fulfillment of a contract. In those instances, the processing must be fair. Fairness includes transparency,

and transparency is challenging in the direct marketing ecosystem. There is room for improved transparency in the direct marketing ecosystem. Fairness also requires a series of assessments to determine that data bring value to people and do not cause actual harm. The General Data Protection Regulation ("GDPR") created data protection impact assessments ("DPIAs") to make sure organisations considered both benefits and harms to stakeholders when processing data. Individuals benefit from competitive markets, so it is reasonable to consider whether less competition because of overly cautious interpretations of data protection law creates harms to individuals that are tangible.

As stated earlier, observation has become overly ubiquitous in today's society. The IAF believes that the movement to limit third-party cookies will have some societal benefits in this area. However, even with those changes, the technology and processing behind market segmentation will be complex and understanding that process will not be most individuals' main concern. So, the role of organisations and regulatory agencies becomes more important. Organisations must conduct assessments at almost every stage of the processing and must be able to demonstrate those assessments were conducted in an honest and competent fashion. Regulators most oversee and enforce substantially enough so organisations believe the likelihood of enforcement is high.

The segmentation process uses probability to segment individuals into cohorts of those likely to do something and those that are not likely to do so. Segmentation logically fits into the GDPR's definition of profiling. The GDPR requires consent where the profiling has legal and similarly significant effect. It is IAF's view that a lack of individual awareness of the robustness of the processing alone does not meet the test of being a similarly significant effect. Similarly, significant effect may come from the actual use of insights to make decisions. DPIAs are designed to identify similarly significant effects, justify or mitigate them, and document the outcome. The IAF sees indications in the Draft Code that the ICO is leaning in the direction of finding that the processing of data for segmentation has significant impact on the individuals the data pertains to. The impact on the societal value brought by direct marketing by requiring knowledge discovery to be subject to consent would be negative and therefore have a negative impact on individuals. The IAF comments explore these issues.

Not all Direct Marketing is Highly Risky

Guidance needs to follow the basic premise of effective regulation in a digital age: controls should be proportional to the risk. The GDPR and the United Kingdom Data Protection Act of 2018 ("2018 ACT") require organisations to differentiate their approach to the use of personal data according to levels of risk in many circumstances. The GDPR specifically differentiates and adds more requirements for profiling where there are legal and similarly significant effects and establishes different requirements for instances where the risk does not rise to that level. The IAF believes that many types of direct marketing are at a lower level of risk.

The Draft Code seems to take the view that marketing activities associated with profiling and automated decision-making necessarily always rise to the higher level of risk. This view leads to unintended consequences. For example, if all direct marketing is deemed to constitute profiling that produces legal or similarly significant effects, then there is less reason for organisations to conduct DPIAs to

demonstrate that risks and interests can be balanced.[1] This result is counter to the risk-based approach of the GDPR.

In the IAF's view, processing of data for analysis only, or "knowledge creation," poses less risk than the application of the resulting knowledge, or knowledge application.[2] By extension, the Draft Code in its present form could preclude the value to people, groups of people, society and market players that could come from permitting truly accountable organisations from using data for knowledge discovery in all settings, not just in direct marketing. The IAF sees in the basic foundation of the Draft Code a tie to the European Union Article 29 Working Party ("WP29") 2017 Guidance on Automated Decision Making and Profiling (" 2017 Guidance") which IAF believes does not accurately reflect the risk-based nature of data protection as provided by the GDPR. All processing must have a legal basis and be fair, but mere processing of data in a secure fashion does not have significant effects. It is the application of the insights that may create significant effects.

Consent is not the Only Legal Basis for Direct Marketing

This result also likely means that consent is the only means to determine the legitimacy of data processing and nullifies the availability of Legitimate Interests as a legal basis to process, if all of its requirements can be satisfied. One purpose of the GDPR was to fix a data protection ecosystem that had become overly reliant on consent, where consent transferred risk from organizations to individuals. The fix is reflected in Article 6 of the GDPR. Specifically, the over-reliance on consent is contrary to Article 6(1) of the GDPR which requires that "Processing shall be lawful only if and to the extent that at least one of the following [legal bases] applies" to each process. Likewise, Section 6(1) does not require that the same legal basis be used for all of the different types of processing performed on the same source data, provided that appropriate notice is given to individuals at the time of initial data collection. The IAF sees the single legal basis as a reflection of the right to privacy, as reflected in the draft ePrivacy regulation, and not the right to data protection. The ICO Guide to the GDPR makes it clear that different legal bases can be used for different processes involving the same data.

Not all Profiling has Legal or Similarly Significant Effects

Organisations may have an effect on individuals when decisions are made and acted on based on the knowledge created, "knowledge application." Those effects may rise to the level of being significant, or not. That is one reason the GDPR requires DPIAs.

Knowledge discovery, or the creation of insights to understand and potentially segment populations, can be "profiling" (the verb). However, to be applied in a manner that can impact an individual, "profiling" usually requires a second step - "attributing those insights to individuals, whether the people are identifiable or not. The result is a "profile" (the noun). Using that profile to send a specific piece of communication to a specific group of individuals is a decision whether it is made by human involvement

[1] The ability of organisations to demonstrate compliance with the risk-based approach of the GDPR is highlighted in the DPIA Section of the ICO's Guide to the GDPR: "This is part of the new focus on accountability and being able to demonstrate that you comply with the GDPR. It is a key element of data protection by design and by default, and also reflects the more risk-based approach to data protection obligations taken throughout the GDPR." Guide to the GDPR.

[2] For a further discussion of knowledge discovery and knowledge application, see Advanced Data Analytics Processing.

or by an automated decision. However, there is a substantial difference in terms of impact across the wide range of marketing decisions. For example, a decision that targets someone who may be interested in a consumer product is materially different from a decision that denies credit, housing, healthcare, or the right to vote in an election. The GDPR is intended to be risk-based; it considers profiling and automated decision making that has a "legal or similarly significant effect" to be of higher risk, requires special notation to the individuals to which it pertains, and grants control rights to individuals. The risk-based nature of the GDPR and accountability mechanisms requires controllers to make numerous determinations as personal data is processed to determine whether profiling is for purposes that trigger the concept of legal or similarly significant effect and further whether the application of the profile to make a decision has legal or similarly significant effect. The IAF was concerned with the direction taken by the WP29 in the 2017 Guidance and said so in its comments on the draft of the 2017 Guidance.

In the IAF's view, the overly rigid 2017 Guidance, conflated profiling and automated decision making, and by attributing the concept of legal and similarly significant effect to all knowledge discovery, has set the basis for requiring consent where it is not effective and has the unintended consequence of stifling the creation of new knowledge. This runs counter to the plain language in the GDPR and the intent that it be risk based.

As noted above, it is the IAF's view that a risk-based approach, as was the intent of a DPIA, would illuminate whether a particular direct marketing program had an impact rising to a standard of legal or similarly significant impact. This standard is not new; internationally, it was first raised in 1970 as part of the United States Fair Credit Reporting Act ("FCRA"). The FCRA covers data used to make substantive decisions. Numerous examples were articulated in the FCRA, such as credit, employment and insurance. Others, such as tenant screening and due diligence on care givers, have been extrapolated. The United States Federal Trade Commission also gave guidance on balancing risk and using data for knowledge discovery and to segment markets. The FCRA guidance said when data was de-identified in an effective manner through an agent of the credit bureau, it could be used for pre-approved offers of credit. While there was some level of privacy risk, the regulatory conclusion was that the lift to competition was greater.

There are circumstances where knowledge discovery for segmentation is being conducted for purposes that may be prohibited by law or may be counter to social norms. A key part of a DPIA is to assess whether the "purpose" of the processing, even in the discovery stage, would be consistent with an assessment of the risk and to identify projects that did not meet the standard of either satisfactorily sufficiently mitigating risks to individuals or meeting the fairness standard required by the GDPR and the 2018 Act. Recent history contains examples of instances where personal data is used to create insights that then targets ads that have significant impact on individuals (e.g. using personal data to target audiences in order to trigger a behavior that limits individuals' rights). There also are examples of persuasive communications, targeted by a profile and actuated based on an automated decision, that are harmful (e.g. telling voters who might vote in an election against the controller's chosen candidate that they might vote via a text when that is not true). The objective behind such knowledge discovery **and** the application of this type of knowledge should be dealt with in an assessment process conducted with integrity and competence and should lead to a decision not to conduct the unfair processing. If profiles indicate insights that are a violation of law or social norms, assessments conducted with

integrity and competence by an accountable organisation would reject their use. Documentation required by the GDPR would create an evidence pattern that could be reviewed by the ICO.

If Direct Marketing Creates Risks, Those Risks may be Able to be Mitigated

The knowledge discovery and the knowledge application discussed here, particularly as it relates to direct marketing, was anticipated by the GDPR. The GDPR speaks to technical and organizational safeguards as a means to mitigate potential risks to individuals. While knowledge creation can create some risks to individuals, they can be mitigated if effective, state of the art technical and organisational safeguards are used. Among those safeguards is pseudonymisation, as newly defined in Article 4(5) of the GDPR with a new heightened standard relative to past practice to help achieve appropriate data protection by design and by default best practices. [redacted] one of the authors of these comments, has joined with others to encourage a discussion of the benefits of GDPR compliant pseudonymisation through the 5th Cookie Initiative (https://www.5thcookie.com/).[3]

More significantly, the IAF is concerned that the Draft Code, by limiting profiling that does not have a legal or similarly significant effect in direct marketing, will create a negative precedent in other instances where personal data are used to develop new insights.

Conclusion

The IAF believes significant reforms are necessary in personal data used for direct marketing, particularly in the AdTech environment. Since the GDPR is risk based, organisations need to make decisions and document them at every step in the direct marketing process. These decisions and this documentation range from judging whether data originated in a fair and legal fashion, whether the data is appropriate to process, what is the legal basis for processing, whether the processing is profiling that will have legal or similarly significant effect, whether the application is automated decision making that will have legal or similarly significant effect, to whether the processing is proportional, legal and fair. These are assessment activities best conducted by a demonstrably accountable organisation with effective oversight. When using personal data to develop new insights, consent usually is not the most effective legal basis for processing.

The IAF appreciates the challenges in drafting a code of practice related to direct marketing, particularly when providing practical guidance to both large and small businesses. However, there are many different types of and approaches to direct marketing. The IAF is concerned that the Draft Code in an attempt to give certainty has eliminated the flexibility provided by the risk-based nature of the GDPR. Neither individuals nor business are benefitted if by providing certainty the advantages of direct marketing, and in particular knowledge creation, are lost.

This letter has discussed the policy concerns the IAF has with the approach taken by the Draft Code. Attached as Appendix A is a discussion of the legal analysis that supports these policy concerns.

Thank you again for the opportunity to comment. For any follow-up, please contact [redacted] at [redacted]@informationaccountability.org.

[3] The 5th Cookie Initiative is not an activity of the IAF

Appendix A – Legal Analysis

Introduction

A basic premise of the Draft Code is that processing for direct marketing purposes when the organisation has not told the individual each specific direct marketing purpose is harmful to the individual because the individual does not expect them. This cannot be the level of transparency that is expected to be provided under the GDPR. Disclosing to the individual that the purpose of the processing is direct marketing and that automated decision-making, including profiling, is used for direct marketing should be enough to give the individual the opportunity to object to direct marketing by opting out. The comments below point out sections of the Draft Code where the premise that the individual's failure to know all the specific purposes of the direct marketing means that the organisation cannot conduct the direct marketing either because it cannot use the legitimate interest basis for processing, because it cannot use the disproportionate effort exception or because **all** automated individual decision-making, including profiling, for direct marketing purposes has a legal or similarly significant effect.

GDPR Article 6(f): Legitimate Interest

The Draft Code states that an organisation might be able to rely on legitimate interest as its legal basis for its direct marketing purposes if it can show the way it uses people's data is proportionate, has a minimal privacy impact and is not a surprise to people or they are not likely to object to what the organisation is doing. According to the ICO, the legitimate interest lawful basis is made up of a three-part test which comprises the legitimate interest assessment. Guide to the GDPR:

- Purpose test – is there a legitimate interest behind the processing? Recital 47 of the GDPR says that direct marketing may be a legitimate interest.
- Necessity test – is the processing necessary for that purpose? The Draft Code says the organisation may need to be more specific about its purposes for some elements of its processing in order to show that the processing is necessary and uses profiling to target the organisation's marketing as an example of when the organisation should be more specific about its direct marketing purposes.
- Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms? The Draft Code rejects the suggestion that direct marketing can be in the interest of individuals (e.g. receipt of money-off products) and recommends organisations focus primarily on their own interests and avoid undue focus on presumed benefits to customers unless the organisation has very clear evidence of customer preferences. The Draft Code also says the organisation should be more specific about its purposes for some elements of its processing in order to weigh the benefits in the balancing test. Also, when looking at the balancing test, the Draft Code provides that organisations should consider factors such as: whether people would expect organisations to use their details in this way, the potential nuisance factor of unwanted marketing messages, and the effect the organisation's chosen method and frequency of communication might have on vulnerable individuals. An example given of when it is very difficult for organisations to pass the balancing test is processing for direct marketing purposes that the organisation has not told individuals about (i.e. invisible processing) and that the individuals would not expect.

As this summary of the legitimate interest section of the Draft Code shows, in order to perform the legitimate interest assessment, the organisation will have to be able to specify the purposes of the direct marketing, but the fact that the individual has not been told about these specific purposes should not mean that the organisation's interest has been overridden by the individual's interests. Recital 47 of the GDPR states that the "interests and fundamental rights of the data subject could in particular override the interests of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect **further processing**." (emphasis added). That it is "further processing" that is the concern and not the disclosure of all purposes is made clear in Article 5(1)(b) of the GDPR which states that personal data must be "collected for specified, explicit and legitimate purposes and not **further processed** in a manner that is incompatible with those purposes . . . ." (emphasis added). Thus, organisations must disclose the purpose for the processing, direct marketing, but do not have to disclose every purpose of the direct marketing, and their failure to do so does not mean that their interests **always** are overridden by the individual's interests, rights and freedoms.

GDPR Article 14: The Disproportionate Effort Exception

The Draft Code paraphrases Article 14 of the GDPR which provides that when an organisation collects personal data from sources other than the individual, i.e., indirectly (e.g. publicly available data and third parties), then the organisation must provide the individual with the information set forth in Article 14 of the GDPR (i.e. provide the individual with a privacy notice). The Draft Code goes on to add that the organisation must provide this information within one month of obtaining the data. However, the GDPR provides that this information does not have to be provided when providing it to the individual would involve disproportionate effort (disproportionate effort exception).

The Draft Code goes on to interpret the disproportionate effort exception. In determining whether an organisation can rely on the disproportionate effort exception, the Draft Code opines that the organisation must assess and document whether there is a proportionate balance between the effort involved for the organisation to give the information and the effect of the processing on the individual. Therefore, according to the Draft Code, if the processing has a minor effect on the individual, the organisation's assessment might find that it is not proportionate to put significant resources into informing individuals, and the more significant the effect the processing has on the individual, the less likely the organisation is to be able to rely on the disproportionate effort exception.

The Draft Code then concludes that an organisation is unlikely to be able to rely on disproportionate effort in situations where the organisation is collecting personal data from various sources to build an extensive profile of an individual's interests and characteristics for direct marketing purposes. The Draft Code reaches this conclusion because individuals will not reasonably expect organisations to collect and use large volumes of data in this way, especially if they do not have any direct relationship with them, and because if individuals do not know about such extensive processing of their data, they are unable to exercise their rights.

There is no authority for the Draft Code's interpretation of "disproportionate effort." Recital 62 of the GDPR states in pertinent part: "it is not necessary to impose the obligation to provide information . . . where the provision of information to the data subject proves to be impossible or would involve disproportionate effort. The latter [disproportionate effort] could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and

any appropriate safeguards adopted should be taken into consideration." Thus, in determining disproportionate effort, the number of individuals to whom the organisation would have to provide a privacy notice, the age of the data, and any appropriate safeguards the organisation had put into place should be taken into consideration. The fact that the personal data collected indirectly is used for profiling does not alone mean that the organisation cannot rely on the disproportionate effort exception. This conclusion is supported by Article 9(2)(j) of the GDPR which states that the prohibition on the processing of special categories of personal data does not apply if the "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes . . . which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject."[4]

GDPR Article 35: Data Protection Impact Assessments

The conclusion that the Draft Code incorrectly interprets the disproportionate effort exception is also consistent with the ICO's position on Data Protection Impact Assessments (DPIA). Article 35(3) of the GDPR requires a DPIA in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data . . . or of personal data relating to criminal convictions and offences . . .; or
c) a systematic monitoring of a publicly accessible area on a large scale.

The ICO additionally requires an organisation to do a DPIA if it plans, among other things, to use profiling or special category data to decide on access to services, profile individuals on a large scale, match data or combine datasets from different sources, collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the nine criteria from the European Guidelines on DPIAs),[5] profile children or target marketing or online services at them. ICO DPIA Guidance

It is important not to conflate the conduct of DPIAs with the determination of whether the disproportionate effort exception applies. As the Draft Code correctly observes, many of the operations that require a DPIA are relevant to the direct marketing context.

The balancing that the Draft Code is trying to achieve through its interpretation of the disproportionate effort exception should be achieved by the conduct of DPIAs by organisations. Under certain circumstances, direct marketing activities should go through the rigor of a DPIA that is not accomplished through determining whether the disproportionate effort exception applies or not.

[4] According to Article 32(1) of the GDPR, pseudonymisation is one of the measures that can be used to ensure a level of security appropriate to the risk.

[5] Evaluation or scoring, automated-decision making with legal or similarly significant effect, systematic monitoring, sensitive data or data of a highly personal nature, data processed on a large scale, matching or combining datasets, data concerning vulnerable data subjects, innovative use or applying new technological or organisational solutions, and processing that in itself prevents data subjects from exercising a right or using a service or a contract

GDPR Article 22: Automated Individual Decision-Making, Including Profiling

Many direct marketing operations also involve automated processing, including profiling, but under Article 22(1) of the GDPR, it is only a resulting decision which produces legal or similarly significant effects that the individual has the right not to be subject to. The Draft Code summarizes profiling as the analyzing of behavioural characteristics of individuals to find out about their preferences, predict their behaviour, make decisions about them or classify them into different groups or sectors; data enrichment as finding out more data on individuals in order to add them to the profile the organisation already holds on them; and data matching or appending as matching the data the organisation already holds on individuals with other contact details that the organisation did not already hold. The Draft Code concludes that

- profiling to better target direct marketing, such as enrichment and data matching or appending, can potentially pose significant risks to the rights and freedoms of individuals because they might not know it is happening or fully understand what is involved, it might restrict and undermine the individual's freedom to choose, it might perpetuate stereotypes, or it might cause discrimination
- direct marketing based on solely automated profiling could have a legal or "similarly significant effect" because there could be situations where it does for example profile to target vulnerable groups or children, target individuals known to be in financial difficulty with marketing about high interest loans, target known problem gamblers with adverts for betting websites, or use profiling to effectively "price-out" individuals of owning a particular product by giving them a much higher price than other people

These conclusions defeat the purpose of doing a DPIA and are more appropriate as examples of conclusions that could be reached in the section of the Draft Code which discusses DPIAs. In that section, the point is made that many of the operations that require a DPIA are relevant to the direct marketing context. It is important that organisations understand that they must conduct DPIAs in order to first determine whether the processing involves profiling or automated decision making and then to determine whether the decision as a result of that processing produces legal or similarly significantly effects. It is only by doing DPIAs that the conclusions can be reached that "profiling to better target direct marketing can potentially pose significant risks to the rights and freedoms of individuals" or that "direct marketing based on solely automated profiling could have a legal or "similarly significant effect.'"

Examples of the types of "legal or similarly significant effects" contemplated are set forth in Recital 71 of the GDPR. They are automatic refusal of an online credit application or e-recruiting practices without any human intervention. Examples of the processing that could give rise to "legal or similarly effects" include 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements. The types of potential risks to be taken into account are discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that results in measures having such an effect. Nothing in Recital 71 suggests that direct marketing has "legal or similarly significant effects."

In any event, not **ALL** profiling for direct marketing purposes has a legal or similarly significant effect. Likewise, not **ALL** direct marketing based solely on automated profiling has a legal or similarly significant effect. The Draft Code should not suggest that merely engaging in profiling for direct marketing purposes or in direct marketing based solely on automated profiling has a legal or similarly significant effect. Articles 13 and 14 of the GDPR require privacy notices to disclose meaningful information about the logic involved in the automated decision-making and the significance and envisaged consequences of automated decision-making on the individual. In making these disclosures, the organisation informs the individual whether direct marketing conducted by automated decision-making, including profiling, has a legal or similarly significant effect on the individual. No further disclosure is required, and the failure to provide further disclosure does not mean there has been a "legal or similarly significant effect."

The Draft Code should facilitate processing and not preclude processing. The GDPR takes a risk-based approach to governance. Requiring organisations to conduct DPIAs to determine whether direct marketing activities, including those involving automated decision-making, including profiling, are highly risky is exactly the risk-based governance in which the GDPR expects organisations to engage.