The Legal Requirements & Technical Concepts of Data Protection

Peter Prescott

2020

i. Introduction

The Troubled Families Program (TFP) was started in 2012, under the authority of the Department for Communities and Local Government, with the aim of focussing resources on helping families struggling with some social problem, and thus achieving measurable impact. A second phase was launched in 2015, and in 2020 funding was extended for another year (Bate et al., 2020).

Its success has been disputed. The initial report produced by the National Audit Office on behalf of the DCLG declared that of 120,000 troubled families involved in the Program, no less than 99% had been "turned around" (NAO, 2016). But an independent report a year later concluded that "no significant or systemic impact could be attributed to the programme" (Day et al., 2016).

In this essay, we do not engage directly with the data regarding whether or not the Program has been effective. Instead we assess the preliminary issue of how to manage the risk of allowing researchers to access the data. We first state the legal requirements regarding data protection in the UK, and then explain how those requirements map onto the context of the TFP. We then explain some of the technical concepts of theoretical data privacy, applying this to the specific case in question. Finally we offer some considered comments and conclusions. My approach is framed in conversation with the actual data protection policy for such research, evidenced by the *Privacy notice for the Evaluation of the Troubled Families Programme* (MHCLG, 2019).

ii. Legal Requirements

The British legal framework governing the processing of personal data is set out in the Data Protection Act (DPA 2018) which applies the standards of the European Union's General Data Protection Regulation 2016 (GDPR, 2016).

The GDPR establishes protection of personal data as a fundamental human right (recognizing that it may need to be balanced against other such rights), including among others the data subject's rights to transparency (Article 12), notification (Arts. 13, 14, 19) access (Art. 15), erasure (Art. 17), and the right to object to the processing of their data (Art. 21). The term 'personal data' is broadly defined (Art. 4) as any information by which a living natural person can be identified.

In general, there should normally be consent for the processing of a person's data, where consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes' (Article 4.11); though it may be 'by a clear affirmative action' rather than necessarily an explicit statement. However, processing without consent is lawful on five other grounds, including if "processing is necessary for the performance of a task carried out in the public interest" (Art.6.1). Where data processing is not based on consent, the controlloer must take into account several factors, including the possible consequences for data subjects, and the existence of appropriate safeguards (Art.6.4).

If some security failure leads to an accidental or unlawful disclosure of personal data, this constitutes a 'personal data breach,' which may be penalized with severe fines (up to ten million euros, or 2% of global annual turnover, whichever is higher Art.83.4).

The required responsibilities differ according to whether a person or agency is a 'controller' or a 'processor'; the former bearing primary responsibility. The controller is the one who 'determines the purposes' (Art. 4.7) of the dat processing; the 'processor' merely processes data as instructed on behalf of the controller. In a given data situation there may be multiple persons who are jointly controllers of the data.

iii. The Context

For example, consider a social worker working for a Local Authority (LA), who asks for the names and dates of birth of all the members of a family with five children from an out-of-work father, who was recently released from prison and is now receiving the Jobseeker's Allowance. So long as she is acting under instructions from the LA, the social worker is a *processor* on behalf of the LA, which is the *controller*. The father is the single *respondent* to the request for data, but all members of the household are independent *data subjects*. If the children are under sixteen, then their father may give consent on their behalf (Art.8), the others must each be notified that their data is now being processed by the LA.

Suppose the social worker then gives that information to the LA's system and database administrator, who uploads the data to a encrypted database hosted in the cloud (Hashemi et al., 2013) by Amazon Web Services (AWS), which requires multi-factor authentication (for example, a password, and a authentication code texted to a given phone number). The sysadmin is another processor, as is AWS.

To decide whether this family should be considered 'Troubled' the LA contacts the local police, to ask if the Police National Computer has any record of criminal behaviour by the family's children; the local school, to find out if school attendance is (un)satisfactory; and the Jobcentre, to confirm the details of out-of-work benefits. The police, the school, and Jobcentre are all controllers of the respective data which they keep. The specific individuals involved in the necessary communication are all processors. This data-sharing is done without specific consent, which is justified on the basis that its purpose is to prevent future crime and disorder, and to support and protect children, according to the advice given by the Department for Communities and Local Government (DCLG, 2012).

The DCLG, renamed in 2018 the Ministry of Housing, Communities and Local Government (MHCLG), contacts the LA asking for the names, addresses and dates of birth of all individuals involved in the TFP to be passed on to the Office for National Statistics (ONS). ONS will then ask the Department of Education (DfE), the Department of Work and Pensions (DWP), and the Home Office (HO) to provide whatever data they have on those listed. The linked data is first *de-identified* so that the specific names, addresses and dates of birth are not attached to the other data. The data is then kept securely and made accessible to a small number of security-checked researchers. These steps are described in the MHCLG's *Privacy Notice* (MHCLG, 2019).

The Privacy Notice assures the reader, in urgent bold font, that this means "no individuals will be identifiable in any published reports or anything shared with MHCLG." We now consider some concepts in the science of data privacy to assess whether this claim is true.

iv. The Science of Data Privacy

To begin with, we consider whether and why anything more is necessary to protect personal data than to remove the specific identifiers of those included in the dataset. Indeed, why not then release the Troubled Families Program data openly, so that the effectiveness of the scheme can be analyzed by whoever might be willing or able. Isn't the government committed (BIS, 2014) to the principle of 'open data by default?' And after all, we have already used the term 'de-identified' for such an action.

While this is the appropriate technical term (the term 'pseudonymization' is equivalent), it only signifies that the data can no longer be attributed to a specific data subject *without the use of additional information*. And this is not a constraint that can be assumed: a nosy neighbour might easily know the number of children in the family, the ethnic group, the accomodation type, and the fact that one of the children often played truant. This is known as a *linkage attack*, and these details are what Samarati & Sweeney (1998) call *quasi-identifiers*. They suggested the use of *generalization* to achieve *k-anonymity*: that is, for any attribute possessed by some individual in the dataset, there are at least k other individual instances of that attribute.

Unfortunately, this too is insufficient. Suppose nosy neighbour Nora were to find out about the open Troubled Families dataset, and see what hitherto unknown information it might reveal to her. She searches the database for families with five children, and finds that of twenty thousand families on the Program, only two hundred have that number of children. Of those two hundred, she queries those with a record of non-attendance at school, of which there are ten – all of which also have a record of youth criminality. In spite of the fact that her queries did not return any unique records, Nora has now discovered a juicy piece of information which she did know previously, and a privacy breach has occurred.

Machanavajjhala et al. (2007) call this the *homogeneity attack*, since the success of Nora's attack on the family's data confidentiality is a result of the homogeneity of five-children families with a record of school non-attendance. They then perform a probabilistic analysis of the difference between an adversary's prior and posterior beliefs due to information learned from a dataset, and suggest the focus be put on ensuring the published data is *uninformative* – that is, it provides the adversary with little additional information beyond their existing background knowledge. To do this, they suggest the notion of ℓ-diversity, which requires that every query returns a block with at least ℓ well-represented values for any sensitive attribute.

But as a strategy for making it safe to release microdata, this too fails. Narayanan & Shmatikov (2008) explain how any large sparse dataset can be de-anonymized, demonstrating the effectiveness of their strategy on the Netflix Prize dataset. 'De-anonymized' not so that every individual identity was revealed, but so that some individuals were matched to publicly available IMDB ratings, thus unveiling their entire Netflix movie rating history, and thereby suggesting particular previously private and clearly sensitive political, religious and sexual preferences. Three months after the Netflix Prize concluded, an in-the-closet lesbian mother sued Netflix for privacy invasion: Netflix settled privately with undisclosed terms (Singel, 2010).

So openly releasing generalized microdata for something with as much potential sensitivity as the Troubled Families Program is clearly not viable. What about perturbing the data by adding random noise? Dwork & Rothblum (2016) suggest a cryptographic approach to data privacy, which she calls *differential privacy*. Acknowledging the *Fundamental Law of Information Recovery*, that there is always a tradeoff between privacy and the usability of statistical databases (Dinur & Nissim, 2003), they offer a mathematical formula for generating the necessary level of noise to guarantee whatever level of probabilistic privacy security is required. By definition this excludes microdata release and is only applicable to queries. Unfortunately, while the mathematics may be rigorous, Bambauer et al. (2014) explain that adding this noise would mean "the great majority of analyses would produce results that are beyond absurd," rendering the research worthless and the data unusable.

It is for these reasons that Elliot et al. (2016) advise that the focus be shifted from considering the mathe-

matics of datasets in themselves, to a more pragmatic consideration of actual data *environments*, in which the risks of processing the data are assessed in context, and appropriate and proportionate plans made to deal with possible breaches if and when they occur.

v. Conclusion

I end with some comments on the MHCLG's chosen data protection strategy: to restrict analysis of the TFP to a small number of cleared researchers in a secure lab after first de-identifying the data; but not – on my reading of the explanation offered in their *Privacy Notice* (MHCLG, 2019)– adding any further privacy-protecting noise. This seems to strike the right balance between carefully limiting the possibility of there being a breach of some very sensitive data, while also protecting the precision and accuracy of the data necessary if researchers are to be able to draw conclusions clear and robust enough to withstand fiercely politicized critique.

The claim offered in their *Privacy Notice* that "no individuals will be identifiable in any published reports or anything shared with MHCLG" seems to be technically true – the described flow of data means that although MHCLG is the data controller requiring LAs to pass on sensitive data, it is all being processed by ONS and other government departments until after accredited researchers have produced their concluding report. But it certainly seems that the MHCLG is not being entirely frank about the possibility that individuals will be identifiable in the data examined by ONS researchers in the secure facility. This would seem to be an example of "concerns about causing unnecessary worry by drawing attention to confidentiality risks" (Elliot et al., 2016).

References

Bambauer, J., Muralidhar, K., & Sarathy, R. (2014). Fool's Gold: An Illustrated Critique of Differential Privacy. *Vanderbilt Journal of Entertainment and Technology Law*, *16*(4), 701–756.

Bate, A., Bellis, A., & Loft, P. (2020). The Troubled Families Programme. House of Commons.

BIS. (2014). Open Data Strategy 2014-2016. Department for Business Innovation & Skills.

Day, L., Great Britain, & Department for Communities and Local Government. (2016). *National evaluation of the Troubled Families Programme: Final synthesis report*. London: Dept. for Communities and Local Government.

DCLG. (2012). The Troubled Families programme: Financial framework for the Troubled Families programme's payment-by-results scheme for local authorities.

Dinur, I., & Nissim, K. (2003). Revealing information while preserving privacy. In *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems - PODS '03* (pp. 202–210). San Diego, California: ACM Press. https://doi.org/10.1145/773153.773173

Dwork, C., & Rothblum, G. N. (2016). Concentrated Differential Privacy. *arXiv:1603.01887 [Cs]*. Retrieved from http://arxiv.org/abs/1603.01887

Elliot, M., Mackey, E., Tudor, C., & O'Hara, K. (2016). *The Anonymisation Decision Making Framework-Mark Elliot,*. UKAN Publications.

GDPR. (2016). General Data Protection Regulation (GDPR) Compliance Guidelines. *GDPR.eu*. https://gdpr.eu/.

Hashemi, S., Monfaredi, K., & Masdari, M. (2013). Using Cloud Computing for E-Government: Challenges and Benefits, *7*(9), 8.

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data*, *1*(1), 3–es. https://doi.org/10.1145/1217299.1217302

MHCLG. (2019). Privacy Notice for the Evaluation of the Troubled Families Programme.

NAO. (2016). *The Troubled Families programme update* (p. 36). National Audit Office.

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)* (pp. 111–125). https://doi.org/10.1109/SP.2008.33

Samarati, P., & Sweeney, L. (1998). Generalizing data to provide anonymity when disclosing information. In *In Proc. PODS* (p. 188).

Singel, R. (2010). NetFlix Cancels Recommendation Contest After Privacy Lawsuit. *Wired*.