Dear Wilf,

DATA PROTECTION BILL: RE-IDENTIFICATION OFFENCE

I committed during the debate on Wednesday to follow up in relation to some questions you had concerning the application of the Government’s new defence for security researchers in relation to the re-identification offence in clause 171. (Clause references below are references to the Bill as amended on Report.)

Terminology

I am afraid I do not share your concern regarding the Bill’s use of the term ‘de-identified’. It is defined in clause 171(2)(a) as “process[ing personal data] in such a manner that it can not longer be attributed, without more, to a specific data subject”. Clause 171(2)(b) defines re-identification as the reversal of that process. This seems to me to be a logical approach.

Intention to cause damage or distress

Clause 172(2)(b) states the subcondition of the researcher re-identifying data without the intention to cause, or threaten to cause, damage or distress to “a person”, where “person” refers to legal persons (including both individuals and organisations). You were concerned that this subcondition could “be used against researchers to threaten or shut down their work”.

Lord Ashton of Hyde
Parliamentary Under Secretary of State
4th Floor
100 Parliament Street
London SW1A 2BQ

020 7211 6000
www.gov.uk/dcms

Lord Stevenson of Balmacara
House of Lords
London
SW1A 0AA

stevensonw@parliament.uk

MC2018/00592/DC
15 January 2018
I can offer some reassurance on this point. The defence will be available to all researchers who abide by the conditions in this clause, including that they did not intend to cause harm or, indeed, distress. It would ultimately be for a court to decide whether that was the case. That an organisation, or indeed a data subject, has merely asserted (without supporting evidence) that the researcher’s intentions were malicious is unlikely to influence the court’s opinion. Similar, the fact that a given re-identification did in fact cause distress would not by itself be evidence that the researcher intended to cause that distress.

72 hour time window

Clause 172(3) requires the researcher to “notify[y] the Commissioner or the controller responsible for de-identifying the personal data... without undue delay, and, where feasible, not later than 72 hours after becoming aware of it.” This language replicates that of Article 33 of the GDPR (notification of a personal data breach to the supervisory authority).

I agree that the 72 hour window represents prompt notification. However, there is, as you put it, significant “elasticity”. I would point not only to the “where feasible”, but also to the “after becoming aware of it”. In addition, I would stress that the clause does not require a detailed dossier to be presented within the 72 hour time window, only notification that attempts to re-identify the data has been successful. The Government anticipates that notification will be the start of a conversation, not an end product in of itself.

Public interest

Clause 172(2)(c) requires the researcher to demonstrate that the re-identification was justified as being in the public interest. Article 6 of the General Data Protection Regulation (GDPR) requires that at least one of the processing conditions listed be met for processing to be lawful. One of these provisions is that the processing was carried out in the public interest, a condition already stated in the main re-identification clause. As I said in debate, the intention of the new clauses is to provide defences for researchers acting in good faith rather than protecting those acting with harmful intent, and one of the ways to distinguish between these intentions is to be acting in the public interest. The researcher will be well placed to meet this test if they satisfy the other conditions in this clause.

Transparency

You asked whether there should “not also be a parallel responsibility, for example, on companies to properly and transparently anonymise the data” (Hansard, vol 788, col 280).

The requirements of the GDPR (particularly Articles 5 and 32) should encourage more data controllers to consider de-identification as part of their broader cybersecurity arrangements. While the Government would encourage controllers to be as transparent as possible about the decisions they take, we would be hesitant to place direct obligations on controllers to publish their de-identification processes, as this may discourage controllers from undertaking de-identification in the first instance. In addition, we would be concerned that a broad brush requirement that applies equally to all controllers may make it easier for criminals to find and attack vulnerable databases.
I am copying this letter to interested Peers, Baroness Williams of Trafford, and Baroness Chisholm of Owlpenn. I will also place a copy in the House library.

Best wishes

Lord Ashton of Hyde
Parliamentary Under Secretary of State