EDITORIAL

Bulgarian Data Hack Provides a Timely Warning of Data Breaches to Come

In June this year the database of the Bulgarian National Revenue Agency was hacked: the personal data of up to five million individuals (in a country with a population of seven million) are understood to have been stolen.[1] Although the hack apparently took place in June, it wasn't until mid-July that it was disclosed, when various emails to press outlets brought the loss of data to public attention. The fact that the Bulgarian tax authorities seem to have been unaware of the loss of data, or unaware of their duty to notify those whose data has been lost, is itself extremely worrying. Reports say that the data included the names, addresses and social security information of up to five million individuals. Further reports suggest that the data included details of taxable income, loans, health insurance payments etc. The Bulgarian Minister of Finance has apologized in Parliament for the loss of personal data.

In mid-July a twenty year old cyber security expert was arrested and charged with the unlawful accessing of the data, though subsequent reports suggest that he may have been released. There are suggestions that the individual may have been acting with good intentions to disclose the weakness of the security surrounding the protection of data on the Bulgarian Government website. However, subsequent reports state that much of the data is now available for purchase on the dark web, which somewhat contradicts the suggestion that the hacker was acting out of good motives. Other reports suggest that the hacker was trying to find information on leading politicians and VIPs in Bulgaria; another report is that the hack originated out of the country and was in retaliation for the announced decision to purchase fighter aircraft from the US.

This incident might have skipped the attention of persons outside Bulgaria, except for those interested in the protection of personal data. No doubt those affected in Bulgaria will have been concerned. However, one can say that everyone should be concerned about this incident, and see it as a warning of a much greater danger that presently exists. This particular incident impacted almost the entire adult population of a country of seven million people. However, there are dangers from the gathering of information about taxpayers by revenue authorities that potentially put at risk the personal data of a much larger number of people.

The hack of the Bulgarian Revenue Agency's data follows on after a history of events involving the theft or accidental disclosure of data by various revenue authorities. In the past these have involved the UK and Italian tax authorities, amongst others. In June 2018 it was disclosed that the personal data of over 80,000 individuals held by the Canada Revenue Agency might have been accessed without authorization in the previous twenty-one months.[2] The data loss in Bulgaria, however, is by far and away the most serious.

Government databases, including those of the revenue authorities, are perhaps the most tempting databases from the point of view of hackers, criminal groups, or even non-benign governments. Often the data contains critical information such as names, addresses, social security numbers, and bank account details. Much of that data has a potential value that may last over a number of years: individuals cannot change their date of birth; may not be able to change their social security number; and are unlikely to change their address in the short-term. Once the data is leaked, it could potentially be used against an individual for years into the future.

In particular, the hacking of the Bulgarian Revenue Agency's data may be seen as a warning and a call to action over the Automatic Exchange of Information (AEOI) under the Common Reporting Standard (CRS). The OECD has implemented AEOI under the CRS since 2018. More than

Notes

[1] The data hack has been reported in a number of press sources. For some of the articles *see* the following: M. Santora, *5 Million Bulgarians Have Their Personal Data Stolen in Hack*, The New York Times (17 July 2019), https://www.nytimes.com/2019/07/17/world/europe/bulgaria-hack-cyberattack.html (accessed 2 Aug. 2019); I. Kottasová, *An Entire Nation Just Got Hacked*, CNN (21 July 2019), https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html (accessed 2 Aug. 2019); *'Wizard' Hacker Charged After Financial Records of Nearly Every Bulgarian Exposed*, The Guardian (18 July 2019), https://www.theguardian.com/world/2019/jul/18/wizard-hacker-charged-after-financial-records-of-nearly-every-bulgarian-exposed (accessed 2 Aug. 2019).

[2] M. Scotti, *Canada Revenue Agency Logs 2,338 Privacy Breaches in Just under 2 Years*, Global News (14 June 2018), https://globalnews.ca/news/4273925/cra-privacy-breaches-searches-documents/(accessed 2 Aug. 2019).

ninety jurisdictions are now participating, and in June 2019 the OECD announced that information had been exchanged on forty-seven million offshore accounts.[3] The standard requirements of the CRS are that, for each account, information should be supplied as to the name, address, jurisdiction of residence, date of birth and tax reference number of the account holder, together with information about account number, account balances and income credited to the account.[4] This includes, potentially, some of the most valuable information that could be sought by hackers, criminal groups and non-benign governments. It is not clear if the lost data in Bulgaria included any that had been received under CRS.

The potential dangers of the lack of adequate data protection surrounding the CRS have been warned about for years. Many of the warnings have been issued by the former Article 29 Data Protection Working Party (which has become the European Data Protection Board since the entry into force of the General Data Protection Regulation (GDPR)). In a letter of 21 June 2012 the Article 29 Working Party already warned about the failure to comply with data protection standards of the agreements to implement the US Foreign Account Tax Compliance Act (FATCA).[5] On 18 September 2014 the Article 29 Working Party issued a further letter warning of the failure of the CRS to implement data protection safeguards.[6] On 4 February 2015, the Working Party issued a statement on the automatic exchange of information for tax purposes, emphasizing the need to provide additional data protection safeguards.[7]

It is difficult in the light of the Bulgarian data theft not to see the OECD's CRS as a disaster simply waiting to happen. The pooling of data under the CRS presents both an immensely attractive target for criminal groups and non-benign governments, as well as a potential data weapon of mass destruction. Is it simply a matter of time before the head of the OECD's Centre for Tax Policy and Administration, or the head of the OECD itself, has to go public to admit that the personal data of perhaps as many as fifty million individuals worldwide (with the number increasing year by year) has been compromised?

The question that one may ask is what will happen after such an announcement. From the point of view of the individuals concerned, it is hard to know what they can do. They may demand that their government issues new tax identification codes, as the old codes will have become compromised. They will have to change bank accounts. They may well demand compensation from the banks that provided the data and that knew in many cases that the revenue authorities were applying inadequate data protection. They may demand compensation from the revenue authorities; they may demand compensation from the OECD who set up the system.

The OECD itself seems already to have considered the scenario of a major loss of data: discussions with officials suggest that they are planning to point the finger at governments who insisted that the OECD developed the CRS system, despite the dangers of data loss. However, it was the OECD that implemented the CRS system, and has to bear responsibility.

Given the damage potentially caused to large numbers of individuals, it will be interesting to see whether, along with fines, criminal charges might follow. With continuing questions being raised over the legitimacy of the OECD to act as the leading organization in international taxation, there must be a real question mark whether the organization can weather a major data breach arising from the creation of the database as part of the CRS.

In recent months we have seen data breaches affecting thousands and sometimes even millions of individuals. However, the Bulgarian incident is the first where the personal data of almost the entire adult population of a country has been hacked from a revenue authority. Taxpayers cannot refuse to supply personal information – some of it highly sensitive – to tax authorities. It appears that we cannot stop AEOI, and no one seems to be able to persuade the OECD or governments of the danger they are creating. All we can do is contemplate what life will be like when our names, addresses, dates of birth, tax codes and account numbers are available to malign forces. Going forward, how will we be able to confirm that transactions are genuinely authorized by us, and not by some malign force that has accessed data hacked from the CRS database or from the database of a revenue authority which received this under AEOI?

Philip Baker
Queen's Counsel, Field Court Tax Chambers, Gray's Inn;
Visiting Professor, Oxford University.
email: pd@fieldtax.com.

Notes

[3] OECD, *Implementation of Tax Transparency Initiative Delivering Concrete and Impressive Results* (7 June 2019), https://www.oecd.org/tax/automatic-exchange/news/implementation-of-tax-transparency-initiative-delivering-concrete-and-impressive-results.htm (accessed 2 Aug. 2019).

[4] *See* OECD, *Common Standard on Reporting and Due Diligence for Financial Account Information* (OECD Publishing 2014) s. I, A.

[5] *See* Art. 29 Data Protection Working Party, *Letter to Mr. Heinz Zourek, Director General of Taxation and Customs Union, European Commission*, Ref. Ares(2012)746461 (21 June 2012), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf (accessed 2 Aug. 2019).

[6] *See* Art. 29 Data Protection Working Party, *Letter on OECD Common Reporting Standard*, Ref. Ares(2014)3066381 (18 Sept. 2014), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140918_letter_on_oecd_common_reporting_standard.pdf.pdf (accessed 2 Aug. 2019).

[7] Art. 29 Data Protection Working Party, *Guidelines for Member States on the Criteria to Ensure Compliance with Data Protection Requirements in the Context of the Automatic Exchange of Personal Data for Tax Purposes,* 175/16/EN WP 234 (16 Dec. 2015), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp234_en.pdf (accessed 2 Aug. 2019)