PSNI and UK voter breaches show data security should be taken more seriously

Publication Date: 2023-08-11

Author: Dan Milmo

Section: Technology

Tags: Data and computer security, Data protection, Freedom of information, Northern Ireland, Internet safety, Electoral Commission, analysis

Article URL: https://www.theguardian.com/technology/2023/aug/11/psni-voter-breaches-data-risks-taken-more-seriously

“It’s brutal. People are wondering if they should resign, or move house, or get fortified gates. You can feel the anger.” The comment from a former officer in the Police Service of Northern Ireland (PSNI) underlines the real-life consequences of an all-too frequent occurrence: a data breach. The UK data watchdog received reports of more than 9,000 personal data breaches last year but the vast majority do not generate public debate, perhaps because the impact is not immediately obvious or the population has become inured to a degree of data loss as an everyday cost of modern digital life. Two incidents this week will have made people think again about what is happening with their data. On Tuesday the PSNI, in a bungled response to a freedom of information (FoI) request, released an Excel spreadsheet containing details of more than 10,000 officers and employees. It was published on an FoI website called WhatDoTheyKnow for about two and a half hours before the PSNI realised the error and had it removed. On the same day, the Electoral Commission revealed it had been hit by a cyber-attack resulting in the perpetrators accessing the names and addresses of anyone in the UK registered to vote between 2014 and 2022, equating to the data of 40 million people. The security threat implicit in the PSNI breach is clear, particularly after the chief constable said on Thursday that dissident republicans claimed to possess some of the information. In February, masked gunmen seriously wounded a senior officer in Omagh, County Tyrone. A PSNI board member said this week that further attacks may follow in the wake of the breach. The consequences for the breach at the Electoral Commission, an independent body that oversees UK elections, are less clear. It says it does not know whether the data, primarily reference copies of the electoral registers, has been downloaded. It also said its email system was breached, meaning any data contained in emails to the commission – such as email addresses, images of documentation and phone numbers – could have been taken. The identity of the cyber-attackers is not known, but the commission has described it as a “complex” attack, and former UK spy heads have said Russia, with its record of attempted electoral interference, is a strong suspect. Working on the assumption that the electoral register copies have been taken, some experts say the data could be combined with other available data to profile users and potentially target them with, for instance, artificial intelligence-generated disinformation around election time. Harjinder Lallie, a senior academic in cybersecurity at the University of Warwick, described the information exposed in the commission hack as potential building blocks for a manipulation campaign, operated by a hostile state, that could be carried out via email, post, WhatsApp groups or social media platforms. “As far as state actors are concerned, the building blocks to enable them to build [disinformation] campaigns are names and addresses. It helps identify people in terms of race, possibly in terms of their financial circumstances, and if combined with other means of data gathering, such as social media profiles, state actors can use that information to build neo-electoral campaigns," he said. The commission has reassured voters about the integrity of the largely paper-based electoral system and said that much of the data exposed was "already in the public domain", for instance people, organisations and companies can already buy the open electoral register, which contains the same information. While some experts have said the data could be allied with the power of generative AI – tools that can mass produce plausible text, images and even voice – to make and send misleading communications at scale, others said this would be ambitious, even for a hostile state. John Hultquist, the chief analyst at the cybersecurity firm Mandiant, said this week that intrusion into an electoral network was "not tantamount to manipulation of the vote". He added, however, that the data could be targeted for different reasons, such as "assembling this information into a database that can be used to identify, track and even exploit persons of interest". Personal information is available publicly (on social media profiles, for instance) or on the dark web, the term for areas of the internet accessible only via a specialised web browser. A cursory check on sites such as https://haveibeenpwned.com/ can show whether people's emails, and other data, has been exposed in breaches. Caroline Carruthers, who runs a data consultancy and is a former chief data officer at Network Rail, said data on people could be available from high-profile breaches, such as that of British Airways in 2018, or from legitimate sources, such as data brokers who compile data about individuals from a number of sources – including the open electoral register – and sell it to third parties. She said social media profiles alone could offer a trove of information. Carruthers recounted a former East German national showing her a secret police report of a dinner party he attended that was limited to a sheet of paper, and she compared that with a friendship group on Facebook discussing a meal she recently attended that contained far more detail. "There was so much more potentially useful information on Facebook than there was in the Stasi report." Carruthers said she hoped the PSNI and Electoral Commission incidents galvanised people's attitudes towards protecting their data from commercial and criminal misuse. "I would really hope this is a wake-up call. I have grave concerns about how we don't take our data, and what it is being used for, seriously enough."