Jane's

Growth of privately held data increases risk of espionage

[Content preview – Subscribe to **Jane's Intelligence Review** for full article]

The breadth and depth of data held by private technology companies are increasing at unprecedented rates. *Anjuli RK Shere* and *Neil Ashdown* examine the changing landscape and how nation-states might target these companies for intelligence collection

Key Points

- The collection of diverse datasets by technology companies is facilitating more powerful inferential analysis about populations and individuals.
- This trend has increased the risk of corporate misuse of this data and of these companies being targeted by threat actors, including nation-state intelligence agencies.
- An effective response to the nation-state threat will most likely require more thorough and innovative staff vetting, a task for which not all technology companies are currently prepared.

Google's self-insert into the healthcare sector has refocused attention on the data giant's access to personal electronic health records and any wider repercussions. The company announced its acquisition of the popular biometric monitoring wearable manufacturer Fitbit on 1 November 2019. Days later, on 11 November, details of a new project with the moniker 'Project Nightingale' were released. Nightingale – a collaboration between Google and Ascension, one of the world's largest Catholic and non-profit healthcare institution networks – was initially unannounced until the *Wall Street Journal* released a report on 11 November 2019 detailing the project and an anonymous whistleblower leaked hundreds of images of internal documents about the initiative in a Dailymotion video that has since been taken down.

In the video and in a 12 November 2019 interview with the *Guardian* , the whistleblower expressed their concern that patients and doctors had not consented to the collection and analysis of comprehensive private medical data. The information shared with Google by Ascension includes, but is not limited to, allergies, diagnoses, and hospitalisation histories – all of which is accompanied by patient names, dates of birth, and home addresses. Julie Clegg, founder and CEO of information security companies HRDN Labs and Human-i Intelligence Services, told *Jane's* that "biometric and health data […could be] used to direct advertising, manipulate unsuspecting individuals, and even influence entire industries and sectors of society. Even more concerning is the threat of misuse with respect of DNA".

The change means that Google has access to the health data of millions of Americans, spanning 21 states in the United States, which is the largest collection of such information handed to the data controller yet. Clegg told *Jane's* that risks emerged not only from Google's possession of the data, but also its processing and analysis capabilities. "When powerful monopolies such as Google gain access to the most personal and private information of citizens, it is not necessarily the breach of personal data that is most concerning, rather the technology that will be developed around that data to manipulate and control not the only messaging in the present, but the direction of nations in the future."

A stock image of the London skyline overlaid with a conceptual graphic intended to suggest the theme of cyber security. Based in London and operated by GCHQ, the National Cyber Security Centre provides advice on cyber-security threats. (Getty Images/alexsl)

1744771

In response to the project's public disclosure, Google released a blog post on 11 November 2019 asserting that its focus was threefold: building Ascension a cloud-based infrastructure, improving Ascension communications and productivity through G Suite (Google's online tools), and creating other, unspecified tools for "doctors and nurses to improve care" through consolidation of patient records. This final point is potentially the most concerning to privacy advocates. Although it would theoretically lead to more efficient and successful healthcare, access to comprehensive health records could also allow Google to mine "emergent medical data" using its artificial intelligence systems. Yale Law School-affiliated fellow Mason Marks described emergent medical data as "a new

type of medical information that is not protected by existing privacy laws" in an October 2017 essay, and specifically linked the concept to the acquisition of Ascension in a November 2019 article on the website Slate, noting that that emergent medical data was "health information inferred by artificial intelligence from mundane consumer behavior". Google's move also aligns with the so-called "extraction imperative" explored in US scholar Shoshana Zuboff's 2019 book *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* , which notes that companies such as Google exponentially expand their data collection activities for predictive purposes to ensure continued profitability and market domination.

[Continued in full version…]

(573 of 2532 words)