Running Rings

Colin Challen

Before the post of North Yorkshire's Police, Crime and Fire Commissioner was abolished in May 2024 – to make way for a new executive mayor – the incumbent offered residents in certain postcode areas, assumed to be at more risk of crime, free Ring doorbell video cameras. These currently sell for upwards of £80. I decided to have one, and it is now fitted. At the very least I no longer anticipate having to get up from the sofa to answer the door to Jehovah's Witnesses. But should I be nervous about becoming a police intelligence gathering service? An accompanying leaflet invites me to register my camera with digitalevidence@northyorkshire.police.uk. Here I learn

> You can register your CCTV cameras or video doorbells on our secure digital evidence management system, NICE Investigate. It's a quick and easy process. By registering you will be set up to send us footage, which we can use to catch criminals. You'll be helping to keep your property and community safe.

NICE Investigate is a Digital Evidence Management System (DEMS) created by NICE Systems (UK) Ltd. That company is part of a largely Israeli/American business started in 1986 which now has a turnover in billions and has become one of Israel's largest corporations. Its CEO is Barak Eilam[1] a former member of the Israeli Defence Force. As with many companies whose primary purpose was gathering and interpreting consumer information, it has used its advanced technological expertise to sell systems to state actors.

The same is true of Amazon, which owns Ring. In 2021 Amazon was contracted by GCHQ to hold data in the Amazon Web Services (AWS) cloud. Following a report in the *Financial Times*, the website *Silicon* reported

> The contract has highlighted data sovereignty concerns, given that a vast amount of the UK's most secret data will be hosted by a single US tech company. However, the FT reported that despite AWS being an American company, the British data will be held in the United Kingdom, according to those with knowledge of the deal. Amazon will not have any access to information held on the cloud platform, those people told the FT. The idea of the AWS contract is that top secret data can be held securely and will allow personnel within the UK intelligence agencies to

[1] Companies House, accessed 13th November.

> easily share data from overseas field locations. It will also allow power specialist apps such as speech recognition which can "spot" and translate particular voices from hours' worth of intercept recordings. The deal will also allow GCHQ, MI5 and MI6 to conduct faster searches on each other's databases.[2]

In the same report:

> Ciaran Martin, who [in 2020] stepped down as head of the UK's National Cyber Security Centre told the FT the cloud deal would allow the security services "to get information from huge amounts of data in minutes, rather than in weeks and months". And Martin dismissed suggestions that the system would affect the amount of information held by intelligence agencies. "This is not about collecting or hoarding more data," he said. "The obvious business case is to use existing large amounts of data more effectively."

I doubt we can place much faith in the last remark. It is generally accepted that the sheer amount of data is doubling every two years or so. Not least, I suspect, from the proliferation of Ring cameras and the like. AI storage and analysis systems developed by large private companies can be bought 'off the shelf' to cope with the volume, saving state intelligence agencies the development costs. The AWS/GCHQ deal is apparently worth between £500 million to £1 billion over 10 years. AWS and other tech giants (all the familiar names) are doing similar deals around the globe. This trend suggests that the insertion of the private sector into intelligence gathering, storage and analysis will supplant the state's own capacity. What was once seen as a clandestine activity solely conducted by the state is now being outsourced at an alarming rate.

In the report of the AWS/GCHQ deal it was said that 'details of the deal are secret and were not intended to be made public.' No doubt it is not only top secret but also 'commercially confidential', so well protected, e.g. from parliamentary scrutiny. Questions must be asked as to the quality of vetting and scrutiny of private company employees – are GCHQ's standards up to scratch? The Parliamentary Intelligence and Scrutiny Committee (ISC) had this to say in 2022 (redacted):

> 69. Over the past year, the Committee has been made aware of two incidents that raise questions regarding GCHQ's security culture and systems.

---

[2] <https://shorturl.at/zpxbq> or <https://www.silicon.co.uk/e-regulation/governance/amazon-web-services-wins-contract-from-uk-intelligence-agencies-423607>

> 70. In late 2022, GCHQ wrote to the Committee to inform it about an ongoing investigation into ***, caused by ***.[The response to this incident was code-named Operation ***] Investigations concluded that *** has had a significant effect on ***. GCHQ concluded that, as per its equities process, it had no option but to *** to ensure that *** an unacceptable cyber-security risk.
>
> 71. The incident raises concerns regarding GCHQ's approach to recruitment and vetting, as well as the stringency of *** protocols in place to ***. The Committee is particularly concerned with regard to ***. The Committee intends to scrutinise this issue further.[3]

Whether these concerns were raised by internal or outsourced recruitment it is impossible to say. Perhaps both, which makes matters rather worse. The Committee doesn't appear to have specifically investigated outsourcing, although it is conducting an inquiry into Cloud technologies. However, at this stage we might recall that Edward Snowden was an employee of an outsourced intelligence business – Booze, Allen and Hamilton – and the question is: are private employees more or less likely to go rogue than state employees? And does GCHQ vet all recruits, including American employees of Amazon Web Services? Presumably they may liaise with the CIA/FBI *et al* to check people out. That activity would be just the kind of thing already privatised on the other side of the pond. Some have gone so far as to suggest the entire CIA should be privatised.[4]

One of the few books on the subject of privatised intelligence, Tim Shorrock's 2008 *Spies for Hire*, made it very clear that the privatisation of intelligence was well advanced in the U.S. to the extent that some agencies employed more outsourced staff than in-house. The danger is that the likes of AWS will be seen as so indispensable to GCHQ that it becomes as integral to its operations as BAE Systems is to the MoD, with all the monopolistic power that entails, with the potential for cost overruns and cosy relations etc. The growing dependence on Cloud services and the potential lack of competition has already been the subject of an inquiry by the Competitions and Markets Authority.[5]

---

[3] HC 287 – Intelligence and Security Committee of Parliament – Annual Report 2022–2023 <https://shorturl.at/RhAun> or <https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-Annual-Report-2022-2023.pdf>.

[4] Tim Shorrock, *Spies for Hire* (New York: Simon and Schuster, 2008) p. 116

[5] Cloud services market study (final report) – Ofcom <https://shorturl.at/dRJ1K> or <https://www.ofcom.org.uk/internet-based-services/cloud-services/cloud-services-market-study/>.

Bearing all this in mind, I think I will choose not to become an unpaid tendril of the intelligence gatherers. It has been asked online whether it is indeed possible to genuinely opt-out if you have a Ring doorbell camera. The answer is not entirely clear. A question posed on Reddit was 'Can Ring see my video?' One answer said

> They absolutely can. Not all staff have access to the tools with which to view the billions of ring videos on their servers, so some CSR [customer service representative] might well say "No no, I can't" — but of course they can be accessed by people who run the system . . . In order to provide access to law enforcement or monitoring services they have to be able to transfer videos as needed. Some perspective is warranted though . . . Ring sold 1.4 million doorbells in 2020. Just doorbells, and just 20 . . . That's not counting all the other years, and not counting other kinds of cameras. There are an absolute asston [sic] of Ring customers out there, so the chances of anyone caring about what's on your recorded footage is minuscule. Unless you have an indoor cam in your bedroom, and you happen to be a celebrity, or a senator, or a public personality of some kind, there's very little chance of someone caring about your particular needle, in the extremely large hay stack.[6]

On the other hand, the Electronic Frontier Foundation (EFF), a digital campaign organisation reported in 2021:

> Almost one year after EFF called on Amazon's surveillance doorbell company Ring to encrypt footage end-to-end, it appears they are starting to make this necessary change. This call was a response to a number of problematic and potentially harmful incidents, including larger concerns about Ring's security and reports that employees were fired for watching customers' videos. Now, Ring is finally taking a necessary step – making sure that the transmission of footage from your Ring camera to your phone cannot be viewed by others, including while that footage is stored on Amazon's cloud.[7]

So, I'll take some comfort from that, safe in the knowledge that if agents of the state wanted to stitch me up, my Ring doorbell wouldn't need to be rung by them.

Colin Challen was Member of Parliament for Morley and Rothwell from 2001 until 2010. He blogs at <http://www.colinchallen.org/blog>.

---

[6] Who can see ring cameras recordings? : r/Ring

[7] 'Amazon Ring's End-to-End Encryption: What it Means' <https://www.eff.org/deeplinks/2021/02/amazon-rings-end-end-encryption-what-it-means>