

## Freedom of Information Act 2000 (FOIA)

### Decision notice

**Date:** 12 July 2022

**Public Authority:** Chief Constable of Kent Police  
**Address:** Police Headquarters  
Sutton Road  
Maidstone  
ME15 9BZ

#### Decision (including any steps ordered)

---

1. The complainant has requested information relating to virus incidents involving Kent Police IT systems 'DropBox' and 'pcloudtransfer'.
2. The Commissioner's decision is that the Kent Police was entitled to apply section 24(2) of FOIA to neither confirm or deny whether the requested information is held.
3. The Commissioner requires no steps as a result of this decision.

#### Request and response

---

4. On 28 December 2020, the complainant wrote to Kent Police and requested information in the following terms:

"In a recent email from a member of police staff I have been informed that "DropBox [and] pcloudtransfer links are blocked by Kent Police Firewall; this position will not change due to previous virus issues."

Please would you disclose all information that is held in relation to these "virus issues", in particular:

- 1) How many virus incidents there have been involving both DropBox and pcloudtransfer, and the dates of those incidents.
  - 2) Which viruses were involved in each incident.
  - 3) What the impact on Kent Police IT systems was, in particular were only individual desktop or laptops affected or were the force's back-end servers / mainframes infected.
  - 4) Did these incidents involve any unauthorised third party gaining access to Kent Police systems.
  - 5) Was any data taken from Kent Police systems without authorisation and if so, what sort of data was involved."
5. Kent Police responded on 2 February 2021, it refused to confirm nor deny whether the information is held and cited section 24(2) and 31(3) of the FOIA.
  6. Kent Police conducted an internal review on 4 March 2021 maintaining its original position.

### **Scope of the case**

---

7. The complainant contacted the Commissioner on 4 March 2021 to complain about the way his request for information had been handled.
8. The Commissioner has considered whether Kent Police is entitled to rely on section 24(2) and section 31(3) of FOIA as its basis for refusing to confirm or deny whether the requested information is held.

### **Reasons for decision**

---

#### **Neither confirm nor deny (NCND)**

9. Section 1(1)(a) of FOIA requires a public authority to inform a requester whether it holds the information requested.
10. The decision to use an NCND response will not be affected by whether a public authority does or does not in fact on hold the requested information. The starting point, and main focus for NCND in most cases, will be theoretical considerations about the consequence of confirming or denying whether or not a particular type of information is held.

11. A public authority will need to use the NCND response consistently, over a series of separate requests, regardless of whether or not it holds the requested information. This is to prevent refusing to confirm or deny being taken by requesters as an indication of whether or not information is in fact held.
12. Kent Police has taken the position of neither confirming nor denying whether it holds any of the requested information in its entirety, citing section 24(2) and section 31(3) of FOIA. The issue that the Commissioner has to consider is not one of disclosure of any requested information that may be held, it is solely the issue of whether or not Kent Police is entitled to NCND whether it holds any information of the type requested by the complainant.
13. In this case, the Commissioner must consider whether or not Kent Police is entitled to NCND whether it holds any information about virus attacks on Kent Police IT systems.

## Section 24

14. Section 24(1) of FOIA states that:

“Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security”.

15. FOIA does not define the term ‘national security’. However, in *Norman Baker v the Information Commissioner and the Cabinet Office* (EA/2006/0045 4 April 2017)<sup>1</sup> the Information Tribunal was guided by a House of Lords case, *Security of State for the Home Department v Reham* [2001] UKHL 47, concerning whether the risk posed by a foreign national provided grounds for his deportation. The Information Tribunal summarised the Lords’ observations as follows:

- ‘national security’ means the security of the United Kingdom and its people;

---

<sup>1</sup> [Microsoft Word - Norman Baker MP v Information Commissioner and Cabinet Office and National Council of Civil Liberties correct \(tribunals.gov.uk\)](https://www.tribunals.gov.uk/cases-and-guidance/microsoft-word-norman-baker-mp-v-information-commissioner-and-cabinet-office-and-national-council-of-civil-liberties-correct)

- The interests of national security are not limited to actions by an individual which are targeted at the UK, its system of government or its people;
- The protection of democracy and the legal and constitutional systems of the state are part of national security as well as military defence;
- Action against a foreign state may be capable indirectly of affecting the security of the UK; and,
- Reciprocal co-operation between the UK and other states in combating international terrorism is capable of promoting the United Kingdom's national security.

16. The Commissioner's guidance on section 24<sup>2</sup> explains that:

"Safeguarding national security also includes protecting potential targets even if there is no evidence that an attack is imminent... We also recognise that terrorists can be highly motivated and may go to great lengths to gather intelligence. This means there may be grounds for withholding seemingly harmless information on the basis that it may assist terrorists when pieced together with other information they may obtain."

17. Furthermore, in this context the Commissioner interprets "required for the purpose of" to mean "reasonably necessary". Although there has to be a real possibility that the disclosure of requested information would undermine national security, the impact does not need to be direct or immediate.

18. Kent Police explained in its submission to the Commissioner that while the requestor is asking about 'Dropbox' and 'pcloudtransfer' specifically, any response could open the gates for questions in respect of other platforms. This would then enable a mosaic effect question, allowing a gradual picture to be formed of what platforms have been allowed, and which have enabled a virus attack. This would undermine Kent Police's ability to safeguard its IT infrastructure.

---

<sup>2</sup> [Section 24 – Safeguarding national security | ICO](#)

19. Kent Police explained that the security services and those engaged in protecting national cyber security will share information with Kent Police in respect of current threats. This may include advice on which software to use, which virus, or hacking threats are of current note, and what actions are required to safeguard IT infrastructures. It explained that simply confirming whether the information is held would undermine the trust with which that information is shared, and ultimately undermine Kent Police's ability to receive and act on notifications from the security services, and those engaged in protecting national cyber security.
20. Kent Police also explained that if it were to confirm whether the information was held it could indicate that Kent Police received such information regarding risk. This would then warn potential attackers that there was a national security awareness of the threat. Conversely, Kent Police explained that denying such information was held would alert potential attackers to a lack of awareness of a potential threat, highlighting vulnerabilities.
21. The Commissioner is satisfied that section 24(2) was applied correctly to the request in this instance. He agrees that if Kent Police was to confirm or deny whether the information was held it would provide attackers with information either of Kent Police's lack of awareness and experience handling a virus attack through 'Dropbox' or 'pCloudtransfer' or that there is a weakness to its IT systems.

### **Public interest arguments**

22. As section 24 of the FOIA is a qualified exemption, the Commissioner proceeded to consider whether or not the balance of the public interest favoured disclosing the information or maintaining the exemption.

### **Public interest arguments in favour of disclosure**

23. Kent Police explained that it recognises that disclosing data reassures the public that Kent Police has a robust cyberattack awareness and acts to protect its IT infrastructure to prevent such threats.

### **Public interest arguments against disclosure**

24. Kent Police stated the following to the Commissioner:

"...it is important to consider that FOI is a release of information into the public domain, something the ICO is very alive to. When considering whether the public interest in withholding the data eclipses that of disclosing, Kent Police must consider what other information may also be available in the public domain and whether release of the

data will add to an overall understanding of the threats faced and the activities underway to prevent such attacks.”

25. Kent Police advised the Commissioner that Britain is now the third most targeted country in the world by cyberattacks from hostile states, according to the UK Government and a high percentage of this was aimed at the public sector.
26. Kent Police stated that if information relevant to the request was held and Kent Police confirmed it was held under FOIA, it would reveal to the public as a whole that there may be vulnerabilities within Kent Police's IT systems which could potentially be exploited through the use of the named application. It also explained that it could confirm that the applications do not hold any risk, and direct malicious actors to target their attentions elsewhere. This would provide an advantage to individuals wanting to hack into Kent Police systems.
27. Kent Police also explained that if information relevant to the request was not held and as a result Kent Police denied that the information was held, the force's ability to neither confirm nor deny whether information is held in the future, for example, where information is held at a later date would be untenable. It explained that this is because neither confirming nor denying whether information is held in such circumstances would actually infer information is held.

### **Balance of the public interest**

28. The Commissioner agrees and recognises that the disclosure of information through FOIA creates transparency and trust between the public and public authorities, in this case reassuring the public that public authorities have a robust cyberattack awareness and secure infrastructure to prevent cyberattacks.
29. Nevertheless, the Commissioner also recognises that there is significant public interest in ensuring that the security of public authorities is not put at risk. In this case there is significant public interest in preventing the disclosure of information which could potentially show vulnerabilities within Kent Police's IT systems.
30. The Commissioner agrees that if Kent Police was to either confirm or deny whether any of the information was held, it could provide an advantage to attackers exposing either lack of experience within the force or providing insight into Kent Police IT systems creating vulnerability for cyberattacks.

31. The Commissioner therefore decided that Kent Police had applied section 24(2) of FOIA correctly in neither confirming nor denying whether the information is held and that the public interest lay in maintaining the exemption.
32. In light of the Commissioner's decision regarding section 24(2) of FOIA, he did not go on to consider section 31(3) of FOIA.

## Right of appeal

---

33. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

First-tier Tribunal (Information Rights)  
GRC & GRP Tribunals,  
PO Box 9300,  
LEICESTER,  
LE1 8DJ


Tel: 0300 1234504

Fax: 0870 739 5836

Email: [grc@justice.gov.uk](mailto:grc@justice.gov.uk)

Website: [www.justice.gov.uk/tribunals/general-regulatory-chamber](http://www.justice.gov.uk/tribunals/general-regulatory-chamber)

34. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.
35. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed  .....

**Laura Tomkinson**  
**Group Manager**  
**Information Commissioner's Office**  
**Wycliffe House**  
**Water Lane**  
**Wilmslow**  
**Cheshire**  
**SK9 5AF**