Intelligence and Security Committee of Parliament
Privacy and Security Inquiry
Response to Call for Evidence

Author:
Dr Kevin Macnish worked at [REDACTED]. He now works as a Teaching Fellow at the University of Leeds. His research interests are in philosophical ethics in the areas of surveillance, security and technology. Dr Macnish is the author of the article on Surveillance Ethics in the *Internet Encyclopaedia of Philosophy* and a forthcoming article on the same subject in the academic journal, *Surveillance and Society*. This contribution is his own and is not submitted on behalf of any organisation.

Executive Summary

- There is no balance to be struck between privacy and security. Surveillance involves harms which go beyond privacy at the individual and collective level, and requires a more nuanced approach than is presently the case.

- Forms of surveillance are more or less intrusive depending on their nature and the context in which they are used. A more intrusive form of surveillance may be more discriminating and *vice versa*.

- Surveillance may be necessary, proportionate, and/or discriminating. There are occasions when necessary and proportionate surveillance is not discriminating. In such cases the use of surveillance may still be justified.

- Collection of content is typically more intrusive than collection of communications data ("metadata"). Communications data may still reveal information the communicant would wish to remain private. Deliberately obscured content may make the collection of communications data more intrusive than the collection of content.

Response

1. *What balance should be struck between the individual right to privacy and the collective right to security?*

2. The right to privacy and the right to security are often presented as a balance or zero-sum game. This is not the case. One reason privacy is valuable is because it contributes to security. When we have our privacy respected, we feel more secure and are less open to threats, blackmail, etc. which may be based on aspects of our lifestyle. To diminish privacy therefore involves diminishing security as well. There is hence no straightforward "trade off" between the two.

3. There are additional harms to individuals involved in surveillance beyond privacy, such as fear of being "found out" or exposure to blackmail. This is also true at the collective level, where surveillance may elicit a "chilling

effect". Chilling effects are such that individuals and groups are deterred from engaging in legitimate democratic activity for fear of being monitored by the state.

4. Instead of a balance between rights to privacy and security, a more helpful means of approaching the issue is to consider a number of principles. These include:
    a. cause justifying the surveillance,
    b. intention behind the surveillance,
    c. authority to carry out the surveillance,
    d. necessity of the surveillance,
    e. chance of success of the surveillance,
    f. declaration of surveillance (to the subject of surveillance or an independent arbitrator such as a judge),
    g. proportionality of the surveillance,
    h. discrimination of the surveillance (the harms of monitoring innocents, or the non-liable, in the pursuit of criminals, etc. – the liable).

    If the surveillance fails to meet these criteria then it should not be pursued.

5. *How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras?*

6. There are considerations which should be taken into account for surveillance as such (the ends) and particular forms of surveillance (the means). When considering forms of surveillance three principles should be borne in mind: proportionality, necessity and discrimination. It is often the case that the more intrusive a form is, the more discriminating it is. Hence monitoring phone calls is very intrusive but also very targeted, and so few "innocents" (the non-liable) are affected. By contrast, CCTV is relatively unintrusive but also generally untargeted, and so many non-liable people may be affected.

7. Monitoring internet communications is too simple a description. What precisely is being monitored? IP addresses, e-mail communications data, web sites visited, search terms recorded, e-mail contents, etc. In each case there is a greater or less degree of intrusion. Monitoring web hosts visited, for example, is *relatively* unintrusive. Monitoring the contents of email communications is very intrusive.

8. Context as well as means is essential to establishing how intrusive a form of surveillance is. CCTV cameras can be used more or less intrusively. A CCTV camera over the front door in a High Street McDonalds is not very intrusive. A CCTV camera in one's bedroom is intrusive. The same is true of internet communications. Discovering that a person visits Google daily is not intrusive. Discovering the fact that a person is having an affair is intrusive. There are of course a number of positions between these extremes. Hence it is of limited use to compare forms of surveillance divorced from their context.

9. *To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security?*

10. “Fishing trips” in which large, untargeted trawls of data take place to discover are rarely if ever justified. These involve a significant access to data of non-liable people (i.e. those who have done nothing to merit the attention of the state). Considerable information can be recovered from such trawls, as became evident in the Leveson Inquiry regarding fishing trips carried out by some journalists on celebrities and members of the public. If the state has unfettered access to large data sets, such as communications data (“metadata”) then there is considerable scope for abuse in discovering information that is not pertinent to national security, as well as that which is. The current UK system of requiring ISPs and telephone companies to retain such data rather than the state is hence preferable to the US alternative of the state holding such data. This limits the potential for fishing trips and holds the state accountable for any surveillance that may be carried out on large numbers of non-liable individuals.

11. Surveillance should seek to discriminate between liable and non-liable people to the greatest extent possible. Many forms of communications surveillance will involve the communications of non-liable individuals. This may be between a terrorist (liable) and his physician (non-liable), or the daughter of a terrorist (non-liable) using the family phone to contact her boyfriend (non-liable). To say that the use of communications by non-liable people renders those communications unavailable for surveillance is hence to virtually rule out surveillance as an option. This is clearly not acceptable: surveillance of the terrorist would be morally legitimate, if not morally required of the state.

12. An analogy can be drawn here with firing a weapon in war. As weapons may be more or less discriminating (compare a sniper’s rifle with a cruise missile) so may different means of surveillance. Those means which are comparatively indiscriminate, in war and surveillance, can be seen as leading to “collateral damage”. Just as collateral damage is regrettable but sometimes justifiable in the context of war, so too is collateral damage sometimes justifiable in surveillance.

13. In addition to discrimination, surveillance should also be proportionate and necessary. Proportionality involves balancing the harms to the individual placed under surveillance and any non-liable people affected against the benefits to be gained from that surveillance, i.e. locating relevant information for the securing of the state. If surveillance is proportionate, though, it does not follow that it is necessary or discriminating.

14. Surveillance is necessary if it is the only or the least intrusive means available, to the surveillant of collecting information on a liable person. Surveillance may be necessary but not proportionate (i.e. it may be the only/least intrusive means but the harms associated still outweigh the benefits) or discriminate.

15. Proportionality, discrimination and necessity are mutually independent. One can have one and lack the other two, or have two and still lack the third. There may also be a trade off, as mentioned in paragraph 6, between proportionality and discrimination. This is because more intrusive forms of surveillance tend

to be more discriminating. It is possible and desirable for surveillance to be necessary, discriminating and proportionate.

16. *How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?*

17. The collection of content is typically more intrusive than the collection of data. Nonetheless, the collection of data is not problem-free. If it were not the case that the data contained information not available elsewhere then it would be of little use to the state. Data does contain information which may legitimately be private. The fact that a person is involved in an adulterous affair, for instance, may be revealed through analysis of such data, potentially exposing that person to blackmail. Data also allows for networks of individuals to be re-created from data analysis. That Tom and Harry both call Dick but never each other may indicate that Tom has a relationship with Harry which either Tom or Harry wish to remain unknown. This is obviously beneficial in terms of uncovering terrorist cells or organised crime networks. It is also open for abuse in that legitimate networks may also be uncovered (anti-government protestors, "swingers", alcoholic support groups, etc.) Through this information people may become exposed to blackmail.

18. The collection of content is usually more revealing than the collection of data. Content may reveal intentions, plans, times and dates of planned events, and so on. In such cases content is extremely valuable. Yet content may also be obscured. It may employ code such that the ingredients for a bomb are given code words to appear as if they were the ingredients for a cake (semtex=eggs, detonators=candles, etc.). Content may also be obscured or rendered unreadable by encryption, use of steganography or a number of other dissembling tactics. When the content of a message is obscured that content may reveal little, but the data surrounding that message may be far more revealing.