Professor Richard J. Aldrich

Politics and International Studies, University of Warwick

Summary of key points that might be made while giving evidence

1. Intelligence as a security panacea.
In an uncertain world, increased knowledge has often seemed a security panacea. Whether global challenges are defined in terms of international terrorism, organised crime, disease or indeed demographic and socio-economic change, a common response has been to turn to knowledge-intensive organisations to manage societal risk. Because today security risk is often thought to revolve around individuals as much as states, the data derived from social media, from our travel cards and shopping is at the core of this activity.

2. The changing ownership of intelligence.
Government no longer owns most of this data on individuals. The most important change during the last decade is that "surveillance" has merged with "shopping" and has ceased to be the preserve of specialist state agencies; instead it has escaped out into society. The big collectors of intelligence are now the banks, airlines, supermarkets, ISP providers and telecoms and the cost of storage is decreasing.

3. The future of intelligence.
In the twentieth century intelligence was owned by states and in the last twenty years we have seen ownership move toward corporations. Over the next twenty years we are likely to see this ownership move again towards individuals. Everyone with a mobile phone will become a mini-NSA and political hacktivism may become mainstream. In the digital realm, states will no longer "create" security they will merely co-ordinate and "curate" security with a broader range of providers.

4. Privacy and Secrecy.
The outcomes of these trends are often portrayed as darkly dystopian. Yet, potentially, these developments also offer stronger partnerships and more open styles of governance that will diminish government secrecy and corporate confidentiality as well as privacy. It will be increasingly hard for anyone to do things in secret. This does not mean that governments will have no secrets at all. But they will be deterred from dubious activity by the stronger possibility of disclosure and shorter time scales for declassification.

5. Ambient Intelligence Oversight.
Just like intelligence itself, oversight and the protection of rights is an activity that is becoming increasingly dispersed. The lead elements are no longer formal committees but global civil society, consisting of a broad alliance of whistle-blowers, journalists, academics, campaign groups, lawyers and NGOs – what we might call "ambient oversight". These fluid oversight networks operate unevenly, but have the advantage of mirroring the multinational alliances of the intelligence agencies which have been hard to call to account.

6. Authoritarian states and criminals.
Random revelations by whistle-blowers such as Edward Snowden are not without cost. Perversely, Snowden's revelations seem to have had the unintended effect of accelerating the global volume of spying on individuals, since many regimes envy the capabilities that he revealed. Efforts to prevent the export of surveillance technology to authoritarian regimes have proved less than ineffective. Citizens will increasingly turn to their own national security agencies to offer them some protection against the worst of this malignant activity from authoritarian states overseas, together with cybercrime.

7. End to End Encryption.
A new generation of young cryptographers are now dedicated to promoting end-to-end encrypted communications. The 1990s "Clipper Chip" episode suggests that governments will prove powerless to stop this development in the long term. What we are likely to see is more limited government access to communications *content* and more expansive access to call data (meta data) or geo-locational information. Perhaps a situation where meta-data is more widely available, but content is harder to access, will provide an uneasy truce in the accelerating wars over privacy and secrecy. More importantly it shows us that the parameters of intelligence gathering and surveillance have tended to be driven by technology, not by law, policy or public debate.

8. Preparing for a more Transparent society.
The advent of a world in which everything around us gathers data means that we must prepare for a world in which individuals have less privacy, corporations have less confidentiality and governments are increasingly bereft of secrecy. The challenge is to ensure that knowledge-intensive security promotes a more open, prosperous and sustainable society. We need to ensure that our data is owned horizontally, openly and democratically. We need to think hard about the growing role corporations will play and what the implications are for democratic control over security. An end to widespread spying is unlikely, instead we need much better oversight and regulation that will ensure stronger public confidence and guarantees of proportionate behaviour.