

You are going to read a newspaper article about technology and personal privacy. For questions 13–19, choose the answer (A, B, C or D) which you think fits best according to the text.

## What price privacy?

*Don't blame technology for threatening our privacy: it's the way the institutions choose to use it*

The most depressing moment of my day is first thing in the morning, when I download my overnight batch of emails. Without fail, it will contain dozens of messages from people who, knowing my interest in the subject, write to me describing violations of their personal privacy. Throughout the day, the stream continues, each message in my inbox warning of yet another nail in the coffin of personal privacy. In other centuries, such invasions of liberty would have arisen from religious persecution or the activities of tax collectors. Nowadays, the invasions take place through the use of information technology.

So, when those of us who value personal privacy are asked for their view, we will invariably speak in disparaging terms about such technologies. In an effort to stem the speed and force of the invasion, we will sometimes argue that the technologies themselves should simply be banned. 'Just stop using the cursed technology,' we cry, 'then there won't be any privacy issue.' Of course, things are not so simple. Even the strongest advocate of privacy recognises that technology can offer enormous benefits to individuals and to society. To prohibit a technology on the grounds that it is being used to invade privacy would also be to deny society the benefits of that innovation.

The sensible perspective is that technology does not necessarily have to invade privacy. The reality is that it invariably does. Companies may well argue that customers are prepared to 'trade off' a little privacy in return for better service or a cooler and more sophisticated product. They say that this is a matter of free choice. I doubt that there is any genuine free choice in the matter. Whether I go with Orange or Vodafone is indeed a free choice. But I have no choice over whether my communications data will or will not be stored by my communications provider. They know the location of my mobile and the numbers from which I received calls, and the emails I send are routinely stored by all providers, whether I like it or not.

CCTV also gives me no free choice. Its purpose may be to keep me secure, but I have no alternative but to accept it. Visual surveillance is becoming a fixed component in the design of modern urban centres, new housing areas, public buildings and even, in Britain at

least, throughout the road system. Soon, people will expect spy cameras to be part of all forms of architecture and design. Of course, there is another side to the coin, many technologies have brought benefits to the consumer with little or no cost to privacy. Encryption is one that springs to mind. Many of the most valuable innovations in banking and communications could never have been deployed without this technique.

The problem with privacy is not technology, but the institutions which make use of it. Governments are hungry for data, and will use their powers to force companies to collect, retain and yield personal information on their customers. In recent years, governments have managed to incorporate surveillance into almost every aspect of our finances, communication and lifestyle. While acknowledging the importance of privacy as a fundamental right, they argue that surveillance is needed to maintain law and order and create economic efficiency. The right to privacy, it is always claimed, should not be allowed to stand in the way of the wider public interest. This argument is sound in principle, but there seems little intellectual or analytical basis for its universal and unquestioned application.

When the UK government introduced the RIP legislation in 2000, it originally intended to allow an unprecedented degree of communications interception on the grounds that the dangers of crime on the Internet warranted increased surveillance. At no time did anyone produce much evidence for this crime wave, however, nor did anyone in government seem to think any was required. It was left to an eleventh-hour campaign by civil rights activists to block the more offensive elements of the legislation from a personal privacy point of view. Such lack of prior justification is a common feature of privacy invasion for law enforcement and national security purposes.

As I've said, technology does not have to be the enemy of privacy. But while governments insist on requiring surveillance, and while companies insist on amassing personal information about their customers, technology will continue to be seen as the enemy of privacy.