OXFORD CAMBRIDGE AND RSA EXAMINATIONS
GENERAL CERTIFICATE OF SECONDARY EDUCATION

2431/02/RBI

ENGLISH (Specification 1900)

Unit 1 Non-Fiction, Media and Information (Higher Tier)

READING BOOKLET INSERT

MONDAY 10 JANUARY 2011: Morning
DURATION: 1 hour 45 minutes

SUITABLE FOR VISUALLY IMPAIRED CANDIDATES

INSTRUCTIONS TO CANDIDATES

The material in this READING BOOKLET INSERT is for use with the questions in Section A of the question paper.

The article 'The end of privacy?' is on page 8, at the end of this booklet.

INSTRUCTIONS TO EXAMS OFFICER / INVIGILATOR

Do not send this reading booklet insert for marking; it should be retained in the centre or destroyed.

DC (KN) 11MEP01173 40511

BLANK PAGE

[In this website feature, Unlock Democracy, a civil liberties organisation highlights some of the dangers they consider we faced in 2009.]

UNLOCK DEMOCRACY

ADVERTISEMENT FEATURE

Civil liberties?
Why should I care?

Published and promoted by James Graham on behalf of Unlock Democracy, both at 6 Cynthia Street, London N1 9JF. Printed by Mail News & Media, Blundell's Corner, Beverley Road, Hull, HU3 1XS.

[In the original website feature, the two questions above are presented in large, red lettering, to the right of the picture of a man's face, eyes staring and mouth set in a determined expression.]

Why civil liberties matter

There is a nationwide debate at the moment about civil liberties and whether or not they are being eroded by the authorities. You may be tempted to think that this debate doesn't really apply to you. IT DOES.

National Identity Database will make us more vulnerable

Human fallibility is a bigger threat than the all-powerful state. No computer system is immune from incompetence, vindictiveness or corruption.

YOU SHOULD BE OUTRAGED that technology meant to tackle terrorism and organised crime is now being used to snoop on innocent individuals to see if they leave dog dirt in the street.

YOU SHOULD BE DISGUSTED that at the same time as insisting taxpayers should pay billions of pounds, those in authority are losing our personal data and other sensitive information in the post and on trains.

YOU SHOULD BE INSULTED that the actions of local authorities compromise civil liberties which have been won after centuries of struggle.

YOU SHOULD BE APPALLED that the rule of law is being replaced by the arbitrary power of public officials. No doubt they have our best interests at heart, but this is not making us any more secure; quite the opposite. No country that prides itself on being a democracy should be able to abolish fundamental human rights. No democracy can be considered safe whose freedoms are not encoded in a basic constitution.

IT IS TIME TO LET THOSE IN HIGH PLACES KNOW THAT ENOUGH IS ENOUGH. Please fill in our online petition.

Would you want to be followed, have your phone and internet records gone through and your emails read by a local government inspector simply to check if you live in the right school catchment area?

[This coloured outdoor picture shows several CCTV cameras at the top of a tall pole.]

When the Regulation of Investigatory Powers Act (RIPA) became law in 2001, it was presented as a tool for investigating organised crime and terrorism. These laws allow over 600 public bodies to intercept email, post and CCTV footage without requiring a court order.

Seven years on, however, these laws are being used by local authorities to investigate a whole swathe of petty crime such as dog fouling, littering and misuse of a disabled parking badge. One local authority even used them to spy on a couple suspected of living outside their children's school's catchment area. Things have now got so serious that the head of the Local Government Association, the body which represents local authorities at a national level, issued a statement reminding authorities to use these powers only when "necessary and proportionate to prevent or detect a criminal offence", to avoid alienating the public.

This is the big danger of passing sweeping laws with few checks and balances. Very quickly they get used for other things as well. The government should review these laws, making sure there are proper safeguards and strong punishments for abuse.

A ruthless dictator is unlikely to take control of the UK any time soon. The real danger of the plans for a "database state" is that it will be vulnerable to human error. Putting incorrect information on the database could lead to individuals being investigated for no reason or being denied benefits. There have been numerous incidents over the years where police and civil servants are believed to have illegally sold personal data to journalists and private detectives. The child benefit

records of 25 million people were "lost in the post" by the Revenue and Customs Office. The official inquiry into the debacle described the handling of taxpayer's personal data as "woefully inadequate". It declared the incident to be "symptomatic of a wider problem." Just recently, secret files on terrorism were left on a train by a civil servant. A Member of Parliament was found to have broken data security rules by leaving sensitive data on a computer which was subsequently stolen from a constituency office. By making databases bigger and giving more people access to them, more problems like this are bound to happen. Those in authority are placing too much faith in technology: it can't protect us from human error, only amplify it.

The end of privacy?

Journalist Pete Warren, writing in 2009, expresses concerns about recent developments in mobile phone technology.

Each time you use your phone, data on your habits is stored and could be sold to advertisers.

While people in the UK were worrying about their houses and lives being photographed on Google Street View, Google must have been pleased. For a much more sinister invasion of privacy had gone unnoticed. A week before, Google had, without any fanfare, released eleven software applications for mobile phones that spell a fundamental change in our lives. Among the applications were functions such as text messaging, web browsing, a diary, Orkut – the company's social networking offering – and a program for Google Maps. Innocent enough, perhaps. But, combined, these features would allow Google to know what you are doing all of the time: a massive betrayal of trust that has horrified privacy campaigners.

The mobile phone industry has for years seen the potential for a rich market to develop in location-based services, if only it could get its customers to agree.The industry's aim is to unite information on customers' age, gender, web-browsing habits, home address and buying patterns with a record of their daily movements, and subject that to analysis of people's behaviour. This provides data on you – the customer – so powerful that the companies involved can predict what you are about to do next, and then sell that information to organisations interested in selling things to you.

“Being able to predict what will you do next and so provide you with useful things at that moment is the ultimate goal,” admits Shaun Gregory, the head of 02 Media.

But all this means that people using such services are making one of the greatest surrenders of privacy in history. A former marketing director of SAS, a leading behavioural analysis company, said: “What is going on at the moment is opening a barn door into your personal habits. The value of understanding people’s personal information is enormous – this will allow a form of mind control through advertising to develop. We are at the tip of an iceberg of what is possible. What happens when governments start to demand access to this data?”

These concerns are confirmed by a representative from his former company. “We have been working with all of the big banks and with the mobile industry on what can be achieved from mobile data,” says the UK head of analytics for SAS. “We can also collect data from people’s voices to tell whether they are lying or not, so this gives us further marketing opportunities.”

The mobile phone companies have always had the technology to access your personal information, but data protection rules have stopped them using it because their customers have not given permission for them to do so. Now, worried about a potential decline in revenue, the mobile industry wants to get around those rules. If we can be talked into signing up for our details to be used in mobile advertising, even if we don’t understand what that means, then their ultimate goal will have been achieved.

While the mobile industry is adamant nothing can happen without the customer's permission, users may not realise what they are agreeing to. If you sign up for any Google services, for instance, you are unlikely to realise you are giving permission for all of your data to be used for marketing. The campaign group, Privacy International, is planning to raise the matter with MPs. "People are being told that they are signing up for marketing when in fact they are being opted into a massive surveillance strategy."

Another insider goes even further and claims: "People do not realise the huge potential of this information for controlling our lives. We are sleepwalking into a minefield."

BLANK PAGE