Surveillance et vie privée

Énoncé

Évaluation de fin de première Épreuve écrite

Durée: 2 heures

Le sujet porte sur la thématique « Imaginaires ».

Prenez connaissance des documents A, B et C et traitez le sujet suivant en anglais :

Write a short commentary on the three documents (minimum 300 words): taking into account their specificities, analyse how the documents deal with the themes of surveillance and privacy.

Document A

Outside, even through the shut window-pane, the world looked cold. Down in the street little eddies of wind were whirling dust and torn paper into spirals, and though the sun was shining and the sky a harsh blue, there seemed to be no colour in anything, except the posters that were plastered everywhere. The blackmoustachio'd face gazed down from every commanding corner. There was one on the house-front immediately opposite. BIG BROTHER IS WATCHING YOU, the caption said, while the dark eyes looked deep into Winston's own. Down at street level another poster, torn at one corner, flapped fitfully in the wind, alternately covering and uncovering the single word INGSOC. In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the police patrol, snooping into people's windows. The patrols did not matter, however. Only the Thought Police mattered.

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

Winston kept his back turned to the telescreen. It was safer, though, as he well knew, even a back can be revealing. A kilometer away the Ministry of Truth, his place of work, towered vast and white above the grimy landscape. This, he thought with a sort of vague distaste – this was London, chief city of Airstrip One, itself the third most populous of the provinces of Oceania.

George Orwell, 1984, Part One, chapter 1, 1949

Document B

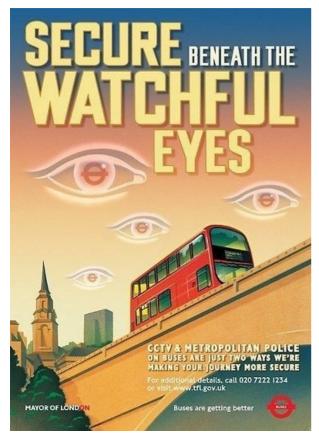
Now the relationship between information and crime has changed in two ways, one absolute, one relative. In absolute terms, people generate more searchable information than they used to. Smartphones passively track and record where people go, who they talk to and for how long; their apps reveal subtler personal information, such as their political views, what they like to read and watch and how they spend their money. As more appliances and accoutrements become networked, so the amount of information people inadvertently create will continue to grow. To track a suspect's movements and conversations, police chiefs no longer need to allocate dozens of officers for round-the-clock stakeouts. They just need to seize the suspect's phone and bypass its encryption. If he drives, police cars, streetlights and car parks equipped with automatic number-plate readers (ANPRs, known in America as automatic licence-plate readers or ALPRs) can track all his movements.

In relative terms, the gap between information technology and policy gapes ever wider. Most privacy laws were written for the age of postal services and fixed-line telephones. Courts give citizens protection from governments entering their homes or rifling through their personal papers. The law on people's digital presence is less clear. In most liberal countries, police still must convince a judge to let them eavesdrop on phone calls.

But mobile-phone "metadata"—not the actual conversations, but data about who was called and when—enjoy less stringent protections. In 2006 the European Union issued a directive requiring telecom firms to retain customer metadata for up to two years for use in potential crime investigations. The European Court of Justice invalidated that law in 2014, after numerous countries challenged it in court, saying that it interfered with "the fundamental rights to respect for private life". Today data-retention laws vary widely in Europe. Laws, and their interpretation, are changing in America, too. A case before the Supreme Court will determine whether police need a warrant to obtain metadata.

Jon Fasman, The Economist online, May 31st 2018

Document C



Official anti-crime campaign Transport for London and the Metropolitan Police, 2002

 $^{\circ}$ 2000-2025, Miscellane