ÉCOLE POLYTECHNIQUE – ÉCOLES NORMALES SUPÉRIEURES

ÉCOLE SUPÉRIEURE DE PHYSIQUE ET DE CHIMIE INDUSTRIELLES

CONCOURS D'ADMISSION 2017 FILIÈRES MP, PC et PSI

ÉPREUVE ÉCRITE DE LANGUE VIVANTE – (XEULCR)

ANGLAIS

Durée totale de l'épreuve écrite de langue vivante (A+B): **4 heures**

Documents autorisés : ***aucun***

⋆ ⋆ ⋆

PREMIÈRE PARTIE (A)
SYNTHÈSE DE DOCUMENTS

Contenu du dossier : trois articles et un document iconographique pour chaque langue. Les documents sont numérotés 1, 2, 3 et 4.

Sans paraphraser les documents proposés dans le dossier, le candidat réalisera une synthèse de celui-ci, en mettant clairement en valeur ses principaux enseignements et enjeux dans le contexte de l'aire géographique de la langue choisie, et en prenant soin de n'ajouter aucun commentaire personnel à sa composition.

La synthèse proposée devra comprendre entre 600 et 675 mots et sera rédigée intégralement dans la langue choisie. Elle sera en outre obligatoirement précédée d'un titre proposé par le candidat.

⋆ ⋆ ⋆

SECONDE PARTIE (B)
TEXTE D'OPINION

En réagissant aux arguments exprimés dans cet éditorial (document numéroté 5), le candidat rédigera lui-même dans la langue choisie un texte d'opinion d'une longueur de 500 à 600 mots.

⋆ ⋆ ⋆

A - Document 1

Sweeping new rules to protect your online privacy

By Brian Fung and Craig Timberg, *The Washington Post*
27 October 2016

Federal officials delivered a landmark ruling in favor of online privacy Thursday, limiting how Internet providers use and sell customer data, while asserting that customers have a right to control their personal information.

Under the Federal Communications Commission's new rules, consumers may forbid Internet providers from sharing sensitive personal information, such as app and browsing histories, mobile location data and other information generated while using the Internet.

The fresh regulations come as Internet providers race to turn their customers' behavioral data into opportunities to sell targeted advertising. No longer satisfied with being mere conduits to the Web, these companies increasingly view the information they collect as a source of revenue.

[...] Ordinary consumers are unlikely to see an immediate impact from the FCC ruling, but privacy advocates had warned that allowing Internet providers to sell the locations, browsing histories and other online data of their own customers could have taken online tracking to a troubling new level, leaving those who wanted to obscure their online activities — or even their physical movements — few options to protect their privacy. "If this was not done, it could have really hard-wired a surveillance infrastructure into the Internet itself," said Jay Stanley, a senior policy analyst for the ACLU.

The new rules, which could face a legal challenge from affected companies, require Internet providers to obtain their customers' explicit consent before using or sharing sensitive data with third parties, such as marketing firms. That could mean dialogue boxes, new websites with updated privacy policies or other means of interaction with companies, which may offer discounts or other incentives to customers who voluntarily consent to online tracking.

The FCC vote also restricts trading in health data, financial information, Social Security numbers and the content of emails and other digital messages. The rules force service providers to tell consumers what data they collect and why, as well as to take steps to notify customers of data breaches.

"It's the consumers' information," said Wheeler, a former cable industry lobbyist who shepherded the rules through a deeply divided FCC. "How it is used should be the consumers' choice, not the choice of some corporate algorithm."

With Thursday's vote, the FCC is seeking to bring Internet providers' conduct in line with that of traditional telephone companies that have historically obeyed strict prohibitions on the unauthorized use or sale of call data.

Internet providers and Republican FCC commissioners complained that limiting the data

collection of Internet providers gave an unfair advantage to other companies such as Google and Facebook that already make billions of dollars collecting data on users and selling it to advertisers.

"There is no lawful, factual or sound policy basis to justify a discriminatory approach that treats ISPs differently from some of the largest companies in the Internet ecosystem that engage in similar practices," said NCTA — The Internet & Television Association, an industry trade group.

But the FCC may have little jurisdiction — or appetite — for regulating the data practices of individual Web companies; Wheeler has repeatedly declined to extend new regulations to the sector.

The different expectations for Internet providers and websites will create confusion among consumers, Republican FCC officials said.

"If the FCC truly believes that these new rules are necessary to protect consumer privacy, then the government now must move forward to ensure uniform regulation of all companies in the Internet ecosystem at the new baseline the FCC has set," said FCC Commissioner Ajit Pai, who suggested that the Federal Trade Commission could accomplish the task.

FTC Chairwoman Edith Ramirez said Thursday's vote would provide strong protections to U.S. Internet users.

"I am pleased that the Federal Communications Commission has adopted rules that will protect the privacy of millions of broadband users," she said in a statement. "We look forward to continuing to work with the FCC to protect the privacy of American consumers." (638 words)

A - Document 2

Privacy no longer a social norm, says Facebook founder

By Bobbie Johnson, *The Guardian*
11 January 2010

The rise of social networking online means that people no longer have an expectation of privacy, according to Facebook founder Mark Zuckerberg.

Talking at the Crunchie awards in San Francisco this weekend, the 25-year-old chief executive of the world's most popular social network said that privacy was no longer a 'social norm'.

"People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people," he said. "That social norm is just something that has evolved over time."

Zuckerberg said that the rise of social media reflected changing attitudes among ordinary people, adding that this radical change has happened in just a few years.

"When I got started in my dorm room at Harvard, the question a lot of people asked was, 'why would I want to put any information on the internet at all? Why would I want to have a website? '."

"Then in the last 5 or 6 years, blogging has taken off in a huge way, and just all these different services that have people sharing all this information."

His statement may not be a surprise, particularly since it helps to justify the company's recent – and highly controversial – decision to change the privacy settings of its 350 million users. But it also represents a remarkable shift from where the Californian company originally started out. Launched in 2004 as an exclusive network for Ivy League students, the site grew in part because [it] allowed people to communicate privately – or at least among small groups of friends.

The constant tug of war between public and private information that ensued led to a series of embarrassing incidents where individuals published information online thinking it was private, only to have it reach the public.

These episodes are partly the result of the way people use Facebook, which has changed its service on several occasions in recent years. Each time the site brings more information into the public domain – and at each point it faces a series of protests and adverse reactions from users.

Moves included the decision in 2006 to introduce the "news feed" – an update of people's activities that is now central to Facebook's service. A year later it launched Beacon, a contentious advertising system that allowed advertisers to track your activities online. That eventually led to the company settling a lawsuit for $9.5m, but it did not prevent it from bringing in new privacy changes in December that one campaign group called 'plain ugly'.

In his talk, however, Zuckerberg said it was important for companies like his to reflect the changing social norms in order to remain relevant and competitive.

"A lot of companies would be trapped by the conventions and their legacies of what they've built," he said. "Doing a privacy change for 350 million users is not the kind of thing that a lot of companies would do. But we viewed that as a really important thing, to always keep a beginner's mind and what would we do if we were starting the company now and we decided that these would be the social norms now and we just went for it."

Not everybody agrees. Marshall Kirkpatrick, of the technology industry blog ReadWriteWeb, said Zuckerberg's statement was "not a believeable explanation" and pointed to the company's complicity in changing the way people think about online privacy.

Meanwhile, others have rejected the idea that younger people, in particular, are less concerned about privacy. Last month Microsoft researcher and social networking expert Danah Boyd told the Guardian that such assumptions often misunderstood the reasons that people put private information online.

"Kids have always cared about privacy, it's just that their notions of privacy look very different than adult notions," she said. "As adults, by and large, we think of the home as a very private space ... for young people it's not a private space. They have no control over who comes in and out of their room, or who comes in and out of their house. As a result, the online world feels more private because it feels like it has more control." (682 words)

A - Document 3

The online surveillance debate is really about whether you trust governments or not

By Jamie Bartlett, *The Telegraph*
6 November 2015

You'll hear lots of lofty language about "national security" and "privacy" over the coming weeks, as the Government's new surveillance bill makes its way through Parliament. It's the third time in the last few years that the government of the day has tried to update surveillance powers.

Each time a predictable war of words breaks out. Those in favour of privacy argue that these powers are Orwellian and put your secrets in jeopardy. On the other the police and intelligence agencies will counter that they are simply trying to update their powers and stop terrorists and criminals hiding online. "It's Orwellian, this internet spying!" shout the civil libertarians. 'But terrorists, and paedophiles!" shout the security people. And, just like in 2001 with the "Communications Data Bill", and in 2008 with the "Internet Modernisation Programme", you have to decide which dystopian camp to throw your lot behind. Is it privacy you don't care about, or security?

[...] In truth, the important distinction in this debate is between those who believe that the law can safeguard your privacy and those who think it cannot. In the one corner are those who think the law can mitigate any dangers to privacy that inevitably comes with surveillance. So the authorities should have the capabilities they need to monitor, hack, surveil, collect – and that any risks to privacy can be managed with more regulations, oversight, scrutiny.

The Home Office are, of course, squarely in this corner, which is why they want a load more powers, but are adding in more restrictions on their application: some judicial oversight on warrants, and a new law that criminalises agencies that abuse their powers. I think the majority of Brits are probably in this camp too, whose view could be best summed up as "let the spies and police do their job, just don't allow them to misuse their power."

The opposition camp is not populated by people who love privacy for paedophiles. It's those who argue that governments tend to misuse powers, and that oversight and scrutiny never really does a decent enough job of limiting possible overreach (and given what we now know, they do have a point). They worry that surveillance always ratchets up: that once governments have a powerful capability they rarely give it up. They suspect that if the government forces companies to collect more data, it will inevitably interest hackers and other bad guys. They don't want "backdoors" to encryption as it would be too readily misused by non-democratic regimes, and perhaps even undermine confidence in the entire net. In short, that the law won't sufficiently mitigate against the privacy risks surveillance creates – and so new powers shouldn't be created. I would put most civil liberties and privacy campaigners in this category, along with almost every journalist and a sizeable minority of the public.

Here's the confusing thing: both have a point. The spies and the police don't really want

to read innocent people's emails. They want to do the job we the public are asking of them, and I think their work is getting more difficult. And the privacy groups don't want to help terrorists, they know eternal vigilance is necessary because intrusive surveillance is easier than ever to sleep walk into. Yet it seems this debate is destined to always be described as "privacy versus security". The problem is this immediately replaces thoughtful discussion with derision, exaggeration and mischaracterisation, and many people probably just hope the bill passes simply to avoid going through the whole ordeal again. That would be a shame of course, because there are more important issues at stake here that are rarely mentioned.

First, it's not clear how long any measures will even work. Thanks in part to Snowden revelations, soon there will be a new generation of easy-to-use encryption services. The net will become more private and also more difficult to censor and monitor, and I think this might require a very real rethink in how we do intelligence.

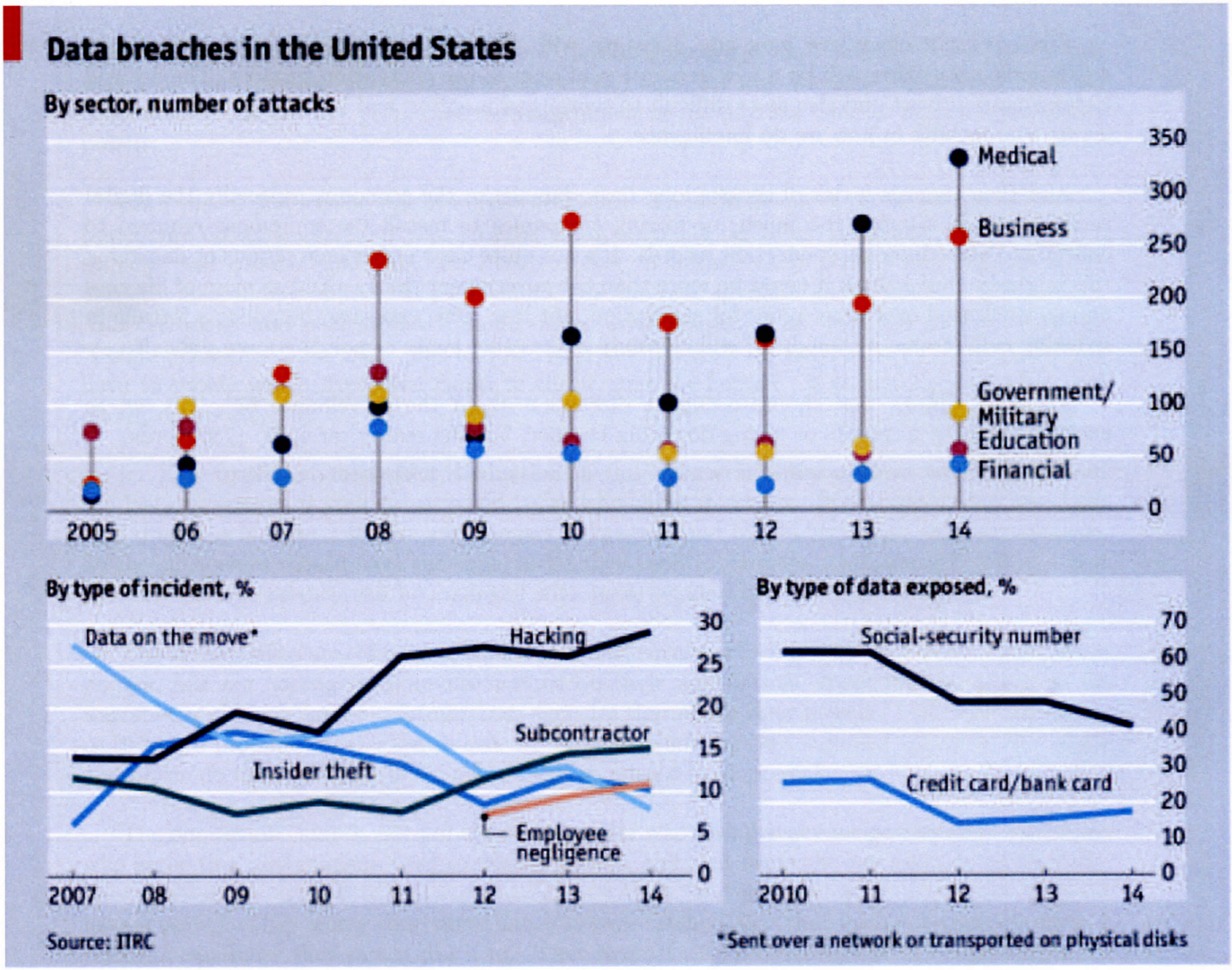
And then there is a risk of serious long term damage to the economy, especially the digital economy, of monitoring too much, or forcing companies to install the equipment required to collect and store internet connection records. It's not quite clear either how serious or damaging this might be, but I think it could be more than the government thinks. And as more of life goes online, we'll need ever more powerful encryption, not less. This can save the police a fortune in reducing cybercrime, although [it] will certainly make other types of policing more difficult.

These are things that should occupy a discussion about the surveillance bill. It's not as exciting catching terrorists or facing down big brother, but the reality rarely is. (788 words)

A - Document 4

Data breaches: The Rise of the Hacker

The Economist
7 November 2015



B - Document 5

WikiLeaks Isn't Whistleblowing

By *The New York Times*
4 November 2016

Whistle-blowing is a time-honored means for exposing the secret machinations of the powerful. But the release of huge amounts of hacked data, with no apparent oversight or curation, does the opposite. Such leaks threaten our ability to dissent by destroying privacy and unleashing a glut of questionable information that functions, somewhat unexpectedly, as its own form of censorship, rather than as a way to illuminate the maneuverings of the powerful.

The latest example of these data dumps comes from WikiLeaks, which is releasing the emails of Hillary Clinton's campaign chairman, John Podesta, in dribs and drabs going back to 2008, when Mr. Podesta was the co-chairman of Barack Obama's transition team.

[...] The hacked emails did provide the public with some notable information. But any benefit of such mass data releases does not undo their harm. And that harm is relevant whether or not the data was stolen by a foreign government seeking to influence this election.

The victims here are not just Mr. Podesta and the people in his contacts list who are embarrassed or compromised. The victim of leaks of private communication is the ability of dissidents to function in a democracy.

Demanding transparency from the powerful is not a right to see every single private email anyone in a position of power ever sent or received. WikiLeaks, for example, gleefully tweeted to its millions of followers that a Clinton Foundation employee had attempted suicide; news outlets repeated the report.

Wanton destruction of the personal privacy of any person who has ever come near a political organization is a vicious but effective means to smother dissent. This method is so common in Russia and the former Soviet states that it has a name: "kompromat," releasing compromising material against political opponents. Emails of dissidents are hacked, their houses bugged, the activities in their bedrooms videotaped, and the material made public to embarrass and intimidate people whose politics displeases the powerful. Kompromat does not have to go after every single dissident to work: If you know that getting near politics means that your personal privacy may be destroyed, you will understandably stay away.

Data dumps by WikiLeaks have outed rape victims and gay people in Saudi Arabia, private citizens' emails and personal information in Turkey, and the voice mail messages of Democratic National Committee staff members. Dissent requires the right to privacy: to be let alone in our vulnerabilities and the ability to form our thoughts and share them when we choose. These hacks undermine that crucial right.

[...] These hacks also function as a form of censorship. Once, censorship worked by blocking crucial pieces of information. In this era of information overload, censorship works by drowning us

in too much undifferentiated information, crippling our ability to focus. These dumps, combined with the news media's obsession with campaign trivia and gossip, have resulted in whistle-drowning, rather than whistle-blowing: In a sea of so many whistles blowing so loud, we cannot hear a single one. (497 words)