CONCOURS CENTRALE•SUPÉLEC

Anglais

TSI 2014

4 heures — Calculatrices interdites

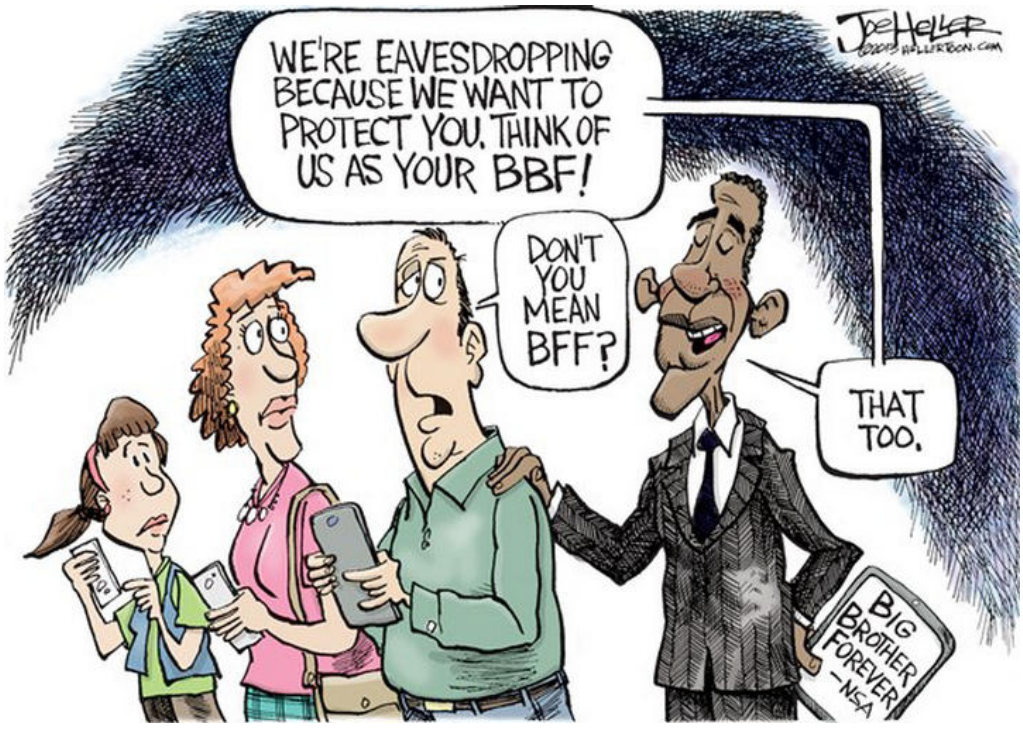
L'usage de tout système électronique ou informatique est interdit dans cette épreuve.

Rédiger en anglais et en 400 mots une synthèse des documents proposés, qui devra obligatoirement comporter un titre. Indiquer avec précision, à la fin du travail, le nombre de mots utilisés (titre inclus), un écart de 10% en plus ou en moins sera accepté.

Ce sujet propose les 3 documents suivants :
- un dessin de presse de Joe Heller ;
- un extrait d'un article paru dans *The New York Times* du 7 juin 2013 ;
- un article paru dans *The New Yorker* le 6 juin 2013, accompagné d'une illustration.

L'ordre dans lequel se présentent les documents est aléatoire.

A cartoon by Joe Heller



published on August 15th, 2013 on *hellertoon.com*

[1] BFF: Best Friends Forever

Making a mountain out of a digital molehill[2]

by Charles A. Shanor, Op-ed contributor[3]
The New York Times, June 7, 2013

The revelations this week that the federal government has been scooping up[4] records of telephone calls inside the United States for seven years, and secretly collecting information from Internet companies on foreigners overseas for nearly six years, have elicited predictable outrage from liberals and civil libertarians.

Is the United States no better than those governed by repressive dictators who have no regard for individual rights? Could President Obama credibly raise human rights issues with his Chinese counterpart, Xi Jinping, at a summit meeting on Friday, if America is running its own vast surveillance state? Has Mr. Obama, for all his talk of ending the "war on terror," taken data mining[5] to new levels unimagined by his predecessor, George W. Bush?

Hold it just a minute.

From what has been made public, we know that the F.B.I., under the Obama administration, used its powers under the Patriot Act to seek these records; that judges with the Foreign Intelligence Surveillance Court approved these searches; and that members of Congress with oversight[6] powers over the intelligence community were briefed about the searches. [...]

It is evident, then, that all three branches of government were involved in the records search [...]. Section 215 of the Patriot Act, which Congress passed after 9/11, governed the executive branch's search authority. Oversight committees were kept in the loop, as Senator Dianne Feinstein, the California Democrat who leads the Senate Intelligence Committee, has confirmed. And the authorizations were approved by life-tenured federal judges who are sworn to uphold[7] the Constitution, including the Fourth Amendment, which prohibits unreasonable searches and seizures. On the surface, our system of checks and balances seems to be working.

We cannot rule out the possibility that the voluminous records obtained by the government might, some day, be illegally misused. But there is no evidence so far that that has occurred. [...]

But shouldn't I be concerned that F.B.I. agents are trampling[8] my rights[...]? As it turns out, the answer is no. The raw "metadata" requested will not be directly seen by any F.B.I. agent.

Rather, a computer will sort through the millions of calls and isolate a very small number for further scrutiny. Perhaps one of the numbers was called by one of the Tsarnaev brothers before the Boston Marathon bombings. Or perhaps a call was placed by a Verizon[9] customer to a known operative of Al Qaeda. The Supreme Court long ago authorized law enforcement agencies to obtain call logs without full probable cause to believe a crime had been committed.

To listen to the contents of any particular call or to place a wiretap[10] on a particular phone, the F.B.I. would have to go back to a judge for a more detailed order, this time showing probable cause sufficient to meet stringent Fourth Amendment standards. Otherwise, the evidence from the call could not be used to prosecute the caller or call recipient. Privacy rights, in short, have been minimally intruded upon for national security protections.

Finally, let's consider the alternative some activist groups and media organizations seek: more narrowly tailored gathering of records, and full transparency after the fact about what kinds of records have been obtained. There are obvious problems with this approach. Let's say the judicial order leaked to *The Guardian* this week had specified the phone numbers about which the F.B.I. had concerns. Releasing those numbers would surely have tipped off[11] the people using those numbers, or their associates, and caused them to change their mode of communicating. Already, there is a real probability that individuals planning terrorist activities are using channels of communication that will not show up in the databases of service providers. If the order revealed more expansively the standards the F.B.I. used to seek broad sets of records, again those seeking to avoid detection for terrorism-related activities could simply change their methods of doing business.

In short, I think I will take my chances and trust the three branches of government involved in the Verizon request to look out for my interest. Privacy advocates, civil libertarians, small-government activists and liberal media organizations are, of course, welcome to continue working to keep them honest. But I will move back to my daily activities, free from paranoid concerns that my government is spying on me.

Charles A. Shanor, a professor of law at Emory, is the author of the casebook "Counterterrorism Law"

[2] To make a mountain out of a molehill: to see a major problem where there is only a minor issue.
[3] Op-ed contributor: an independent writer who contributes articles to a newspaper giving his personal opinions on various subjects, regardless of the newspaper's editorial line.
[4] To scoop up: to pick up.
[5] Data mining: information gathering and analyzing.
[6] Oversight: supervision; to oversee something: to supervise something.
[7] To uphold: to maintain.
[8] To trample: to violate.
[9] Verizon: an American telecommunications company.
[10] To wiretap: to listen in on phone calls.
[11] To tip somebody off: to inform somebody, to warn somebody.

THE NEW YORKER

June 6, 2013

by Jane Mayer

What's the matter with metadata?

Illustration by Matthew Hollister

Dianne Feinstein, a Democrat from liberal Northern California and the chairman of the Senate Select Committee on Intelligence, assured the public earlier today that the government's secret snooping into the phone records of Americans was perfectly fine, because the information it obtained was only "meta," meaning it excluded the actual content of the phone conversations, providing merely records, from a Verizon subsidiary, of who called whom when and from where. In addition, she said in a prepared statement, the "names of subscribers" were not included automatically in the metadata (though the numbers, surely, could be used to identify them). "Our courts have consistently recognized that there is no reasonable expectation of privacy in this type of metadata information and thus no search warrant[12] is required to obtain it," she said, adding that "any subsequent effort to obtain the content of an American's communications would require a specific order from the FISA court."

She said she understands privacy—"that's why this is carefully done"—and noted that eleven special federal judges, the Foreign Intelligence Surveillance Court, which meets in secret, had authorized the vast intelligence collection. A White House official made the same points to reporters, saying, "The order reprinted overnight does not allow the government to listen in on anyone's telephone calls" and was subject to "a robust legal regime." The gist of the defense was that, in contrast to what took place under the Bush Administration, this form of secret domestic surveillance was legitimate because Congress had authorized it, and the judicial branch had ratified it, and the actual words spoken by one American to another were still private. So how bad could it be?

The answer, according to the mathematician and former Sun Microsystems engineer Susan Landau, whom I interviewed, is that it's worse than many might think.

"The public doesn't understand," she told me, speaking about so-called metadata. "It's much more intrusive than content." She explained that the government can learn immense amounts of proprietary information

[12] A search warrant: a document authorizing police search.

by studying "who you call, and who they call. If you can track that, you know exactly what is happening—you don't need the content."

For example, she said, in the world of business, a pattern of phone calls from key executives can reveal impending corporate takeovers. Personal phone calls can also reveal sensitive medical information: "You can see a call to a gynecologist, and then a call to an oncologist, and then a call to close family members." And information from cell-phone towers can reveal the caller's location. Metadata, she pointed out, can be so revelatory about whom reporters talk to in order to get sensitive stories that it can make more traditional tools in leak investigations, like search warrants and subpoenas[13], look quaint[14]. "You can see the sources," she said. When the F.B.I. obtains such records from news agencies, the Attorney General is required to sign off on each invasion of privacy. When the N.S.A. sweeps up millions of records a minute, it's unclear if any such brakes are applied.

Metadata, Landau noted, can also reveal sensitive political information, showing, for instance, if opposition leaders are meeting, who is involved, where they gather, and for how long. Such data can reveal, too, who is romantically involved with whom, by tracking the locations of cell phones at night.

For the law-enforcement community, particularly the parts focussed on locating terrorists, metadata has led to breakthroughs. Khalid Sheikh Mohammed, the master planner of the September 11, 2001, attacks on New York and Washington, "got picked up by his cell phone," Landau said. Many other criminal suspects have given themselves away[15] through their metadata trails. In fact, Landau told me, metadata and other new surveillance tools have helped cut the average amount of time it takes the U.S. Marshals to capture a fugitive from forty-two days to two.

But with each technological breakthrough comes a break-in to realms[16] previously thought private. "It's really valuable for law enforcement, but we have to update the wiretap laws," Landau said.

It was exactly these concerns that motivated the mathematician William Binney, a former N.S.A. official who spoke to me for the Drake story, to retire rather than keep working for an agency he suspected had begun to violate Americans' fundamental privacy rights. After 9/11, Binney told me, as I reported in the piece, General Michael Hayden, who was then director of the N.S.A., "reassured everyone that the N.S.A. didn't put out dragnets[17], and that was true. It had no need—it was getting every fish in the sea."

Binney, who considered himself a conservative, feared that the N.S.A.'s data-mining program was so extensive that it could help "create an Orwellian state."

As he told me at the time, wiretap surveillance requires trained human operators, but data mining is an automated process, which means that the entire country can be watched. Conceivably, the government could "monitor the Tea Party, or reporters, whatever group or organization you want to target," he said. "It's exactly what the Founding Fathers never wanted."

[13] A subpoena: an order to come and be a witness in a court of law.
[14] Quaint: old-fashioned yet charming.
[15] To give oneself away: to reveal one's location by mistake.
[16] A realm: a domain.
[17] A dragnet: a very deep fishing net.