

ESADE

Ramon Llull University

ESADEgeo-CENTER
FOR GLOBAL ECONOMY
AND GEOPOLITICS

E

53

**Book reviews
on global economy
and geopolitical
readings**



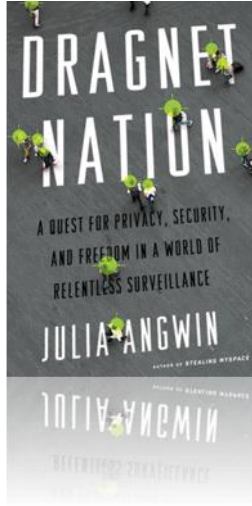
Fundación
REPSOL



Obra Social "la Caixa"



Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance



Angwin, Julia, (2015), St. Martin's Griffin, New York.

"Who is watching you? This was once a question asked only by kings, presidents and public figures trying to dodge the paparazzi and criminals trying to evade the law. The rest of us had few occasions to worry about being tracked. But today the anxious question – "who's watching?" – is relevant to everyone regardless of his or her fame or criminal persuasion. Any of us can be watched at almost any time."

"Surveillance dragnets are inherently unfair. By definition, they capture the innocent and the guilty indiscriminately. In doing so, they create a culture of fear."

Summary

We live in a dragnet nation: a world of indiscriminate tracking in which institutions collect data on individuals at an unprecedented rate. Before the computer age, it was difficult and expensive to track citizens. Governments kept records on exceptional events such as births, weddings, deaths, and property purchases. Companies acquired data about customers when they bought something, or requested a guarantee or loyalty card. In *Dragnet Nation*, Julia Angwin explains how technology has made it easier and cheaper to track individuals during almost every moment of their lives. Moreover, trackers are not only strangers, but include trusted institutions and companies with whom we do business and who should be on our side.

While many sceptics ask what is wrong with hundreds of advertisers and hidden data brokers watching us and collecting our data while we surf the net, the author of *Dragnet Nation* stresses that our data can and will be abused. Today, thanks to information shared on the network, we can be located at any moment, spied on in our own homes, our personality can be stolen, our finances can be hijacked, and we can be subject to police control. Even more worrying, according to Julia Angwin, is the fact that our information is not always stolen, but is sometimes lost – for reasons ranging from incompetence to piracy. And only rarely are companies penalised for losing our data.

In *Dragnet Nation*, the author convincingly explains a simple truth: information is power. Anyone who has a great deal of data about us has power over us. At first, the information age promised to empower individuals with access to previously hidden information. But now the balance of power is swinging towards those large institutions and corporations that took the lead in accumulating vast amounts of information on ordinary aspects of our lives, thereby creating a culture of fear.

For the author the question is simple: do we want to live in a world where we always run the risk of being hacked? A world where we can always be found and cannot keep secrets, etc.? The author firstly explains why we should worry about indiscriminate surveillance. She examines the legal and technical origins of the dragnet nation, the uses and abuses of surveillance, and the impact it is having on individuals and society. Secondly, she explores whether there is any chance of building an alternate world, where we can enjoy the benefits of technology without the constant fear of being hacked. The final – and fully achieved – objective is to move the current debate from ‘Who is watching me?’ towards a more in-depth discussion about ‘Does it matter?’ and ‘What can we do about it?’

The author

Julia Angwin is an award-winning investigative reporter for the independent news organisation ProPublica and author of *‘Stealing MySpace’*. From 2000 to 2013, she reported for *The Wall Street Journal*, where she was part of a team of reporters awarded the 2003 Pulitzer Prize for coverage of corporate corruption. She also led a team that covered online privacy and was a finalist for the 2012 Pulitzer Prize.

Key ideas and opinion

In an attempt to understand the history and origin of mass surveillance, Julia Angwin turns the clock back to **2001**. This was not only the year of the **devastating terrorist attacks** on the United States; it was the year in which the technology industry was stunned by the **bursting of the dot-com bubble**. The author explains how **these two seemingly unrelated events together launched a chain of events that created the legal and technical basis for today’s dragnet nations**. For the American government, the terrorist attacks revealed that their traditional intelligence-gathering methods were not working. And for Silicon Valley, the bursting bubble showed the need to find a new way of making money. Both came to the same answer to their differing problems: namely, gathering and analysing vast amounts of personal data. It is not surprising, therefore, that in May 2006, *USA Today* published an article stating that shortly after 9/11, the phone companies AT&T, Verizon, and BellSouth began giving customer call records to the National Security Agency (NSA).

George W. Bush came under pressure and eliminated some parts of the programme. However, **in 2008, he amended the Foreign Intelligence Surveillance Act in order to restore and legalise wiretapping and immunise the phone companies** against legal action for their previous involvement in potentially illegal programs. In 2012, the Justice Department authorised the National Counterterrorism Center to copy entire databases with information on American citizens: flight records; lists of casino employees; names of Americans who have housed exchange students; etc. There records were routinely examined in a search for suspicious behaviour. **Thus, almost without realizing it, unannounced dragnets have become the new standard.**

Silicon Valley internet companies were accused of not having the metrics to measure the effectiveness of their products, and so began looking for better measurement standards. As a result, **a tool for following users on the net was developed – the cookie**. By 2007, all the Internet giants were in the online tracking business. For example, Google paid \$3.1 billion for DoubleClick, and Microsoft paid \$6 billion for aQuantive – both the acquisitions being companies that build Internet user profiles.

Given this reality, the author of *Dragnet Nation* states with concern that **surveillance is now marked by unsuspected, powerfully computerised, and impersonal tracking. While some commentators believe that this monitoring will make the world safer, others, including the author, fear the arrival of a police state.** To understand the worst case scenario, she visited the best-preserved records from the pre-electronic surveillance era, namely, the **Stasi** secret police archives in Berlin, and compared the records with current commercial operations and government surveillance. The Stasi records included four million East Germans. However, without the advantage of current technology, the mapping of crucial social networks was complicated and not very reliable, unlike the extensive data currently offered by social networks such as Facebook. But the main problem with the Stasi, in the opinion of the author, was the fact that, although it was not very good at gathering in-depth information about each individual, the mere existence of a Stasi record could be a determining factor in being given a job or achieving promotion. **Fear of becoming the subject of a police file generated anxiety and a feeling of mistrust and oppression that was sufficient to make individuals change their behaviour** – either by becoming model citizens or hermits.

Extrapolating this analysis into the current context, **the author wonders to what degree mass surveillance has led to changed behaviour or prevented terrorist attacks.** As an example, she quotes General Keith Alexander, director of the NSA, who declared that telephone tapping and dragging the internet had helped uncover 55 terrorist plots. Although he did not name all the cases, he did mention the case of Najibullah Zazi, who in 2009 was arrested just days before he and his friends intended a suicide bombing in the New York subway. Julia Angwin doubts whether the government needed to use all these tracking techniques to capture Zazi. If Zazi was

E exchanging emails with terrorists under surveillance, a simple search warrant would suffice to monitor their communications. Similarly, once his phone number was known, it is likely that a judge would have approved a simple phone tap.

Angwin therefore asks whether massive surveillance has been worthwhile when the staunchest defenders can only say that it “has contributed to our understanding” of cases “at the margins”. Research published by Jeff Jonas (a researcher at IBM) and Jim Harper (director of information policy at the Cato Institute) concluded that **terrorist acts were not common enough to be identifiable through the large-scale data gathering**. Angwin points out that, at the end of the day, Zazi bought nail polish remover to make his explosive. In comparison, data mining works well for pursuing credit card and insurance fraud, which are more common activities. As stated throughout the book, data mining is used for multiple purposes, from identifying potential terrorist acts to building user profiles for establishing the maximum price a customer will pay for a specific flight (based on their online behaviour pattern and interests).

For the author, in a world where almost everything is monitored, it is easy to feel hopeless about preserving privacy. For that reason, **she decided to try living for a year in the modern world while evading constant tracking**. The process turned out to be exhausting and, for the most part, unsuccessful. She started by building a threat model to identify the main risks to her security – which in her case were indiscriminate online tracking and targeted attacks against journalists and their sources. She then sought to build a defence model after consultation with many sources, from senior government officials to hackers who build anti-surveillance tools.

Her model included a set of operating criteria: not breaking the law; living in the modern world and not disconnecting from technology; using conventional tools that she herself could build, modify, or design; trying to spread no data by using services that do not store data; engaging in data pollution (either by using fake names or providing false information); protecting her traffic (meaning the people with whom she exchanged emails, calls, or instant messages); using communication systems in real time and storing nothing; employing data dispersal (to minimise any damage following possible leaks, data breaches, or government espionage, among others); paying for good programs (in the hope that the programs would continue to improve); requiring transparency disclosure (it is always better if you can see the data that is being stored, and correct or download it); searching for options with the greatest level of privacy (the best example of this practice being to avoid airport body scanners); and finally, not succumbing to fear (because when carrying out all the above measures, it is very likely that a red flag would be raised at the NSA).

The new world in which the author was entering reminded her of the world of dissidents in repressive regimes: a world where quiet conversations in a bar were safer than phone calls, emails, or other electronic communication. **All these measures led**

E

Angwin to identify more than 200 data brokers who gathered data about her life. She then contacted these brokers and asked them to provide a copy of the information they held on her. Only 13 agreed to do so. She also asked companies to eliminate the data they had on her – an approach which usually failed to produce results. Creating a false name, date of birth, address, phone and credit card, and buying series of prepaid cards for phone calls made it difficult to communicate with her contacts. She used a metal-covered wallet to prevent scanning, but discovered that it also blocked her mobile phone's signal. She used software such as Silent Circle to encode her messages, but found that this did not work very well because her contacts had to use the software as well. She installed anti-tracking programs such as AdBlockPlus and NoScript, but found that they conflicted with other applications such as Firefox. She tried to avoid face recognition cameras, which turned to be almost impossible. In general, **she found herself becoming increasingly paranoid as she discovered who was watching her.**

Although the results are discouraging compared to the perseverance of the author in wanting to live in the modern world without being monitored, Angwin learned **some lessons** and explains them to the reader. For example, **disconnect your phone's wifi whenever you are away from home** (to prevent companies stealing information from your mobile phone). The author also emphasises the need to **set secure passwords**, and explains a simple lesson she learned from hackers: create long passwords and avoid simple or single words such as 'password1'. Greater complexity means greater difficulty in discovering a password. Passwords containing many kinds of symbols, letters, and numbers often require more attempts to guess them. Julia Angwin explains that Assange knew the importance of complex passwords, which led him to create the following password for confidential WikiLeaks cables: AcollectionOfDiplomaticHistorySince_1966_ToThe_PresentDay#. To create strong passwords, Angwin recommends Diceware, an online password generating program that enables you to generate passwords from five or six random words that have no connection with your life (and are therefore difficult to guess). She keeps these passwords on a piece of paper that she carries with her, and says that these Diceware passwords can be further strengthened by adding uppercase letters or symbols. It would generally take 800 days to crack such passwords. This approach is particularly crucial for email, which is the key to access the rest of our online accounts, and moreover, a place where we are unprotected from fraud – unlike banks, which do offer protection against fraud.

The author also shows readers how to **replace the Google meta-search engine with a small tool called DuckDuckGo, which has a policy of not retaining user data.** Angwin explained that after months of using DuckDuckGo she found she missed the millions of results produced by Google, and the ease of quickly and intuitively finding the information she was seeking, but she was also made aware just how much Google had been guiding her searches, and that with DuckDuckGo, it was she who guided the

computer. She was also pleased to note that this tool stored none of the information emitted by users' computers – such as IP address and other digital fingerprints.

The main lesson Angwin teaches us in *Dragnet Nation*, however, is the need not to accept indiscriminate surveillance. The author compares the loss of privacy with pollution. Both are results of the exploitation of a resource: land, water, or information. In both cases, it is difficult to attribute responsibility for causing the damage because it is often an accumulation of pollutants or data. In the cases of pollution and privacy, the damage is collective. In the case of pollution, no single individual bears responsibility, yet we all suffer when the air and water are contaminated. Similarly, we all suffer when we live under the fear that companies or the police can use our data against us. In this regard, **the author welcomes the growing movement to make companies responsible for the data they store on individuals.** In fact, the **European Union requires companies to give citizens access to the data they hold on them.** In America, the courts recently seem to be considering whether the dragnet has been too intrusive for its intended aim, whether it has benefited society, and whether it is motivated by racism or prejudice.

According to Angwin, **society should not tolerate indiscriminate surveillance** in the same way that society does not tolerate people who steal without being punished, or bribery, or companies that sell dangerous products. For this reason, **the author calls for greater transparency and accountability with regard to surveillance.** She proposes six questions that should be asked of every dragnet:

- Does the dragnet provide individuals with a legal right to access, correct, and dispute data?
- Are the dragnet operators held accountable for the way the data are used?
- Is the dragnet too intrusive for its purpose?
- Does it benefit society?
- Does it fall into the ugly abyss of racism (or other prejudices)?
- Can it withstand public scrutiny?

With these questions, Angwin expects to find a compromise between those who gladly give their data away and those who choose to live completely outside the technological world. The author is confident that the answers to these questions will enable us to **distinguish between dragnets that are intolerable and unjust – and those we can accept.**