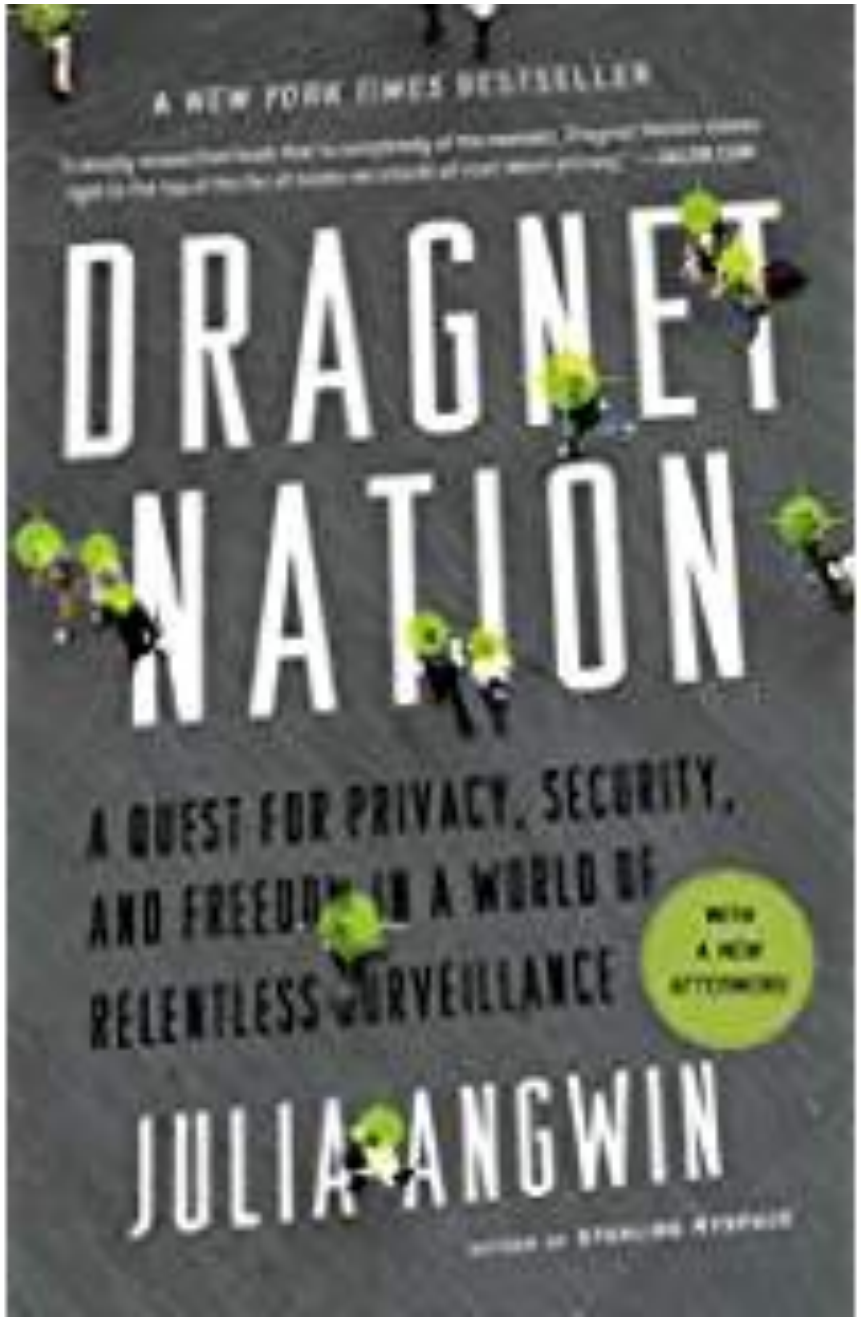
SURVEILLANCE SOCIETY

- Dragnet Nation—Julia Angwin

- BIG Data: A Revolution That Will Transform How We Live, Work, and Think—Victor Mayer-Schonberger, Kenneth Cukier

- The Art Of Invisibility—Kevin Metnick


A NEW YORK TIMES BESTSELLER
DRAGNET NATION
A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE
JULIA ANGWIN

“We are living in a Dragnet Nation—a world of indiscrimi
tracking where institutions are stockpiling data about ind
an unprecedented pace. The rise of indiscriminate tracki
powered by the same forces that have brought us the te
that we love so much—powerful computing on our deskt
laptops, tablets, and smartphones.” (p. 3)

Each of us must now be aware that every bit
information we give out about ourselves is co
filed, and (probably) sold by businesses and
governments (federal, state, and local).

Examples:

Government forms you complete
Emails you send/receive
Texts you send/receive
All telephone numbers called
All data on social media (i.e. photos, friends info, etc.)
Websites you visit
Products you order online
All purchases you make with credit cards
Forms you complete online
Ads you click on
Books you check out from the library
Places you visit (with GPS/cell phone in pocket)
Your digital calendars

Governments around the world—from Afghanistan to Zimb
are snapping up surveillance technology,ranging from “mas
intercept” equipment to tools that let them remotely hack in
people’s phones and computers. Even local and state gove
in the U.S. are snapping up surveillance technology rangin
drones to automated license plate readers…. Local police
increasingly tracking people using signals from their cell ph
4)

Mall owners have started using technology to track shopp
signals emitted by the cell phones in their pockets. Retaile
as Whole Foods have used digital signs that are actually f
recognition scanners. Some car dealerships are using a s
that lets them know which cars you have browsed online,
have given them your email address, before you arrive on
dealership lot.

Cell phone tracking by police is now “as routine as looking fo
fingerprint evidence or DNA evidence.”

Inevitably, phone companies have started selling cell phone
data to a wider audience than just police. In 2013, Verizon sa
would sell a new product called Precision market Insights tha
would let businesses track cell phone owners in particular lo

One of Verizon’s first customers is the Phoenix Suns basketb
team, which wants to know where its fans live. A team
representative said, “This is information that everyone has w
that hasn’t been available until now.”

As more and more data is collected and, apparently, becom
easily accessible, problems arise. Regarding “impersonation
identity theft”, “complaints increased by nearly one-third in 2
up to 369 million from 279 million a year earlier.

Crooks use our personal info for credit card fraud, tax fraud
bogus tax returns seeking refunds), and medical fraud (obta
medical care using someone else’s data.)

Online tracking has fueled a new industry: **data trading**. C
exchanges similar to the stock exchange, advertisers buy
sell customer profiles in millisecond trades. It works like th
when you look at, say, a digital camera on eBay, the Web
is embedded with code from a data exchange such as Blu
Once BlueKai is alerted that you are on the page, it instan
auctions off your “cookie” to advertisers who want to reach
camera buyers. The highest bidder wins the right to show
a digital camera advertisement on subsequent pages that
visit. That’s often why online ads appear to follow you arou

“Personal data is the new oil of the interne
the new currency of the digital world.”

The trackers are deeply intertwined. Governm
data are the lifeblood for commercial data
brokers. And government dragnets rely on
obtaining information from the private sector.

Think about voting forms. Few voters realize that those lists
often sold to commercial data brokers such as Aristotle, Inc

Aristotle combines the voting information with other data to
rich profiles of individuals. For instance, it markets its ability
identify 190 million voters by more than “500 data points” su
their credit rating and size of their mortgage.

And guess who buys Aristotle's enriched data? Politicians, who sometimes using government money. Aristotle crows that "ever U.S. president—democrat and republican—from Reagan to Ob has used Aristotle's products and/or its services." In fact, a 201 report found that fifty-one members of the U.S. House of Representatives bought data from Aristotle using some of their congressional allowance, allowing them to identify their constit by the age of their children, whether they subscribe to religious magazines, or if they have a hunting license.

The term "**the Dark Data Cycle**" refers to the dynamic of government requiring citizens to create data and then selling it commercial entities, which then launder the data and sell it bac the government.

“In today’s world, every choice we make associates us wi
person, a place, or an idea. Visit a political website; you a
associated with its views. Sit in a restaurant near somebo
who is being watched; your cell phone is now part of the
“community of interest” that may be monitored by authorit
These associations are scooped up and entered into
databases where people use them to make predictions al
your future behavior.”

Eric Schmidt, the chairman of Google, wrote in his book The Ne
Digital Age, the rise of “near-permanent data storage” will usher
an era where “people will be held responsible for their virtual
associations, past and present.”

Other authors, even those who are bullish on Big Data, also
express concerns. Mayer and Cukier comment in a section of t
book called “Police Sate 2.0”: ”Everything a regime would need
build an incredibly intimidating digital police state is commercia
available now.”

“So I decided, against all odds, to try to evade the dragnets. I
attempt to avoid being monitored during everyday activities su
reading and shopping. I would obscure my location—at home
while out and about. I would seal my e-mails and texts with th
digital equivalent of hot wax. I would find ways to freely assoc
with people and ideas.” (p.65)

Bruce Schneier in Schneier On Security:

“There’s no such thing as absolute security. Life entails risk, an
security involves trade-offs. We get security by giving up somet
money, time, convenience, capabilities, liberties, etc.”

“I consulted with experts of all kinds—from high-level government officials with security clearances to hackers w build anti-surveillance tools. Each had a different suggestion. ...After many such conversations, I came to re there was no silver bullet. I would have to come up with m own battle plan.”

STRATEGIES

1. “The best way to protect my data is not to give it away.
the best way to do that is to use services that don’t store c

2. Engage in data pollution. “When I can’t minimize my
trail, I can try to pollute it by using fake names and prov
misinformation.” [This was hard for a self-described “Go
Two-shoes.”]

“So I vow to remind myself that the people who require
fill out forms online in order to accomplish simple tasks
always deserve truthful answers.”

3. Regarding texts: “Its not easy to turn off storage of texts
instant messages, particularly because you often can’t con
whether the recipient is storing the information. But, luckily
most voice and video discussions are not stored by default
a result, plain old-fashioned domestic telephone calls are s
one of the most private ways to communicate.”

“I decided to begin my privacy quest by trying to find my data.”

“To find my Google data, I visited the website of Data Liberation F
quirky Google project that lets users download the data that they
stored with Google. Using their “take-out’ menu, I downloaded the
contacts for the 2,192 people whom I have emailed since I started
Gmail in 2006. I also got a few photos I had stored on Picasa (Go
photo service, which I had forgotten I used). And I pulled down tw
documents that I had shared with people using Google Drive (but
204 that had been shared with me by others). ...When I tried to do
the history of websites I had visited, I learned “There is no current
escape from Google Web History.”

I found a bit more information on my Google Dashboard—a page t
contains information about my activity on various Google services
was buried in my Gmail account settings. ...I have had 23,397 e-m
chat conversations on Gmail."

"Strangely, my Web search history wasn't on my dashboard. It was
hidden away in a section of my account called "other tools." There
that Google had been logging my Web searches from the time I op
my account in 2006. Apparently I conduct hundreds and sometime
thousands of Google searches per month. [Her reaction to viewing
was] "This was more intimate than a diary. It was a window into my
thoughts each day."

Facebook was considerably less forthcoming with my data. I clicke
“download a copy of my data,” and Facebook sent me an archive t
was notable for what it did not include, [including] my list of friends
posts, likes, or comments on other people’s posts.

Eventually she discovered that Facebook’s data use policy “stated
explicitly that ‘information associated with your account will be kep
your account is deleted.’”

Later she discovered that this was not true: “in short, it seemed tha
Facebook planned to keep my data—whether or not I deleted it [ar
wasn’t likely to obtain a comprehensive set of my Facebook data a
soon.”

“Getting my data from Twitter was easy. I simply pressed
button labeled “Request your archive.” Twitter promptly s
me an e-mail with a handy Excel spreadsheet containing
2,993 tweets since I opened my account in 2008.”

DATA BROKERS

She interviewed the president of a data broker called TLO.

“Can I see my report?” I asked’

“Sure,” he said.

“In less than a minute I was holding a 4-page report containing
my previous addresses—dating back to the number on my do
room in college: #536B. There was not a single piece of inacc
information in the report.”

“I compiled a list of more than 200 commercial data brokers, a
was pretty sure I hadn’t identified all of them.

The U.S. data business is largely unregulated, which is not the
in most western European countries. Those countries require
data collectors to provide individuals with access to their data,
ability to correct errors in the data, and, in some cases, the rig
delete the data.

After reading the fine print on 212 websites, I learned that only
them offered me chance to see the data they held about me.”

I was shocked that Acxion, the data-gathering giant with annua
sales of $1.1 billion, asked me to send a $5 check as a proces
fee to obtain my data. But I sent it, gritting my teeth. One mont
later, Acxion sent me a nine-page report with my social securit
number, birth date, voter registration, and addresses dating b
to childhood. None of the information that Acxion sells about m
interests was provided. This was particularly galling since Acxi
brags in its annual report that it has more than “3,000 propens
for nearly every U.S. consumer.” One of its main products is th
PersonicX database, which lumps people into seventy “cluster
within twenty-one “life stage groups.”

Finally, I sought to extract my data from the U.S. governme
[She did not try the NSA as “others have tried them and failed.”]

I requested my FBI files and was informed that it had no records for me (phew!) but that this response “neither conf
nor denies the existence of your subject’s name on any wa
lists.”

A database called PNR—Passenger Names Records—used to be a com
database for the airline industry but has been essentially co-opted by the
government since 9/11. “A robust view of my travel was contained in a se
set of documents—thirty-one pages of detailed international travel reserv

My full credit card number was in there several times, as were my e-mail
addresses, my birth date, my passport number, and all of my phone num
work, home, and cell. My fellow travelers’ information was in there as we
husband’s e-mail address, my children’s birthdates, and all our passport
numbers.

It appeared that my corporate travel agency was also contributing inform
the federal government. For a trip to London, the agency sent Customs n
reservation, my corporate credit card number and expiration date, my em
ID number, my department budget code, and an internal code that I was
VIP.”

WHAT TO DO?

Secure your passwords.

“I was reminded of a study that claimed that 38 percent of adults
rather do household chores, such as cleaning the toilet bowl or d
dishes, than create a new username and password.”

Overwhelmed by needing to create and remember many passwo
decided to install **password-management software**” called Ipas
which is “essentially a password vault; you store all your passwor
software. You unlock the vault with a single master password. To
that the passwords are totally secure, they are not stored at Ipass
offices in Canada, but on your machine in an encrypted file.”

“To combat impersonation (a.k.a identity theft) I bought a **shredder** started shredding documents containing personal information.

And I bought a **wallet that blocks radio-frequency identification signals** on my credit cards and passport, which can be skimmed by hackers.”

To ensure that my data would be secure in case of a more serious h bought an **external hard drive** and started backing up my files regu

To foil hackers who might make it into my machine, I **encrypted my drive** (which on a Mac was a one-click operation).

I put a sticker over my Web camera.”

“I installed software called **HTTPS Everywhere**, which ensured that connection to the Internet were encrypted whenever possible.

Instead of relying on my home Wi-Fi router, I plugged my computer hard-wired Ethernet connection. When traveling, I started using a **portable Wi-Fi hot spot** that I carried with me. The connection was sometimes spotty, but it made me feel a lot better than connecting to those intrusive hotel Wi-Fi systems that force your traffic through the system.”

I also set up double-password systems—known as **two-factor authentication**—when it was available.”

Creating strong passwords takes some effort. “I needed a
system where I didn’t have to think. (!yes!)

I found what I needed in a password system called **Dicew**
It is deceptively simple; you roll a six-sided die five times a
use the results to pick numbers from the Diceware word lis

CHAPTER 7:” Leaving Google”

“I don’t dislike Google. In fact, Google has tried hard to be transpare
about surveillance. It was the first big Internet company to start pub
reporting the number of law enforcement requests it received.

But Google has also repeatedly abused users’ trust.

I started by quitting Google search.

To replace Google search, I found a tiny search engine called **DuckDuckGo** that has a zero-data retention policy. It doesn’t store the information that is automatically transmitted by my copter—the I address and other digital footprints.”

She describes a bit of a learning curve, as DuckDuckGo
not have all the automatic features that Google has. Still,
eventually “I had broken free from Google, and the world
still on its axis. I had mastered another service and could
find the information I needed.”

“I really didn’t want to quit using Gmail. But its hard to justify using
email service that admitted to reading my mail. Of course, Google s
that humans aren’t reading my mail. It’s only computers that scan m
email for keywords, and then insert ads based on those keywords.

But that’s what the National Security Agency says about domestic s
too.” (!)

After reviewing a number of alternative email services, she settled
paid version of Thunderbird, called Postbox.

Consider an alternative: PROTONMAIL