The New Panopticon:

the right to privacy in the digital age
Soon, everybody will be able to see everything.

(Ashton 2014)
Privacy in the digital age:

Does email enjoy the same privacy as a letter?

Should a mobile call merit the same protections as one made from a land line?

Can strangers take pictures of me with their cell phones and upload them to the internet for everyone to see?

Today, more and more cell phone users would rather text than talk. Do the privacy protections that attach to phone calls also apply to texting?
This robber would rather text than talk:

Police Add Texting to Crisis Negotiation Arsenal

By THE ASSOCIATED PRESS  MAY 11, 2014, 8:42 A.M. E.D.T.

The suspect in a gas station robbery and 100 mph chase kept pointing his handgun to his head, and police negotiator Andres Wells was doing all he could to keep the man from committing suicide. But he kept cutting Wells' phone calls short.

Then, about 10 minutes after the last hang up, Wells' cellphone chimed. It was a text — from the suspect.

"Please call Amie," the message said, followed by the number of the man's girlfriend.
In his opinion in U. S. v. *Jones*, J. Antonin Scalia notes that in the digital age,

people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks:

People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

Perhaps . . . some people may find the “tradeoff” of privacy for convenience “worthwhile,” or come to accept this “diminution of privacy” as “inevitable,” and perhaps not.

I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.
Warren and Brandeis are reacting to the potential for photography and the press to impact the privacy of private individuals (public figures are subject to different privacy rules).

How do changes in technology continually redefine the boundaries between the private and the public?
In what way can you apply Warren and Brandeis to the age of the internet and the cell phone video?

Michael Richards, who played Kramer on *Seinfeld*, caught here on a cell phone video of his stand-up comedy routine ranting and using the n-word to an audience heckler.

The video went viral, and Richards’ comedy career tanked.
“Don’t tase me, bro.” Student tased by University of Florida police at a John Kerry rally, captured on a cell phone video and uploaded to YouTube, becomes an instant celebrity.

The phrase “don’t tase me, bro,” becomes an instant meme.
Warren and Brandeis note that “the right to privacy disappears upon publication.”

How does that stand up in the context of email, Facebook, Twitter, and other sorts of online activity, where one has—at times—the ability to limit who may read/view/listen to a post? Are privacy controls illusory?

Is that what Mark Zuckerberg and others mean when they claim that modern technology has rendered privacy dead?

In 2013, 4 zettabytes of data were generated worldwide.

That’s 1 billion terabytes.

Big data is not just a buzzword, it’s a force of nature.
Coffee shops are public places, as are Facebook pages. But is the broadcasting of a semi-private conversation by a third party an invasion of privacy?

There were 13 billion internet-connected devices on the planet in 2013: more devices than people.

How does that affect our privacy?
Gotcha: The red-light camera at work in Chicago:
The internet of things monitors our behavior and reports our whereabouts:

Apple’s new iWatch tracks location but also has apps that monitor health (heart rate, steps taken, calories burned) and spending (what you bought, for how much, and where you bought it). Is this simply a convenient feature that users want, another challenge to privacy, or both?
Ashton: Soon “everybody will be able to see everything.”

manufacturer of 220-pound microsatellites, calls the big picture “planetary awareness.” Combining data from sensors on satellite networks with information from things like phones, cars and planes will give us a comprehensive, constantly updating picture of the world. Everybody will be able to see everything from crops growing to traffic jamming to armies invading to icecaps melting. Vanishing airplanes will be a thing of the past.
Blackstone on eavesdropping as a violation of Common Law:

Eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and . . . are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behavior.”

[Commentaries 1769, p. 169]
Stored Communications Act 1986 (when the internet was young and people used it differently) protects digital privacy only on a time-limited basis:

law enforcement needs no warrant to access electronic communications stored on a server for more than 180 days.

It’s like forgetting to pick up the dry cleaning: the law assumes that electronic storage is temporary, and so anything left on a server long-term must have been abandoned.

This law is still in force, used to justify warrantless NSA searches.
NSA Director James Clapper: Surveillance? It’s no biggie.

“What did us in here, what worked against us was this shocking revelation,” he said, referring to the first disclosures from Snowden. If the program had been publicly introduced in the wake of the 9/11 attacks, most Americans would probably have supported it. “I don’t think it would be of any greater concern to most Americans than fingerprints. Well people kind of accept that because they know about it. But had we been transparent about it and say here’s one more thing we have to do as citizens for the common good, just like we have to go to airports two hours early and take our shoes off, all the other things we do for the common good, this is one more thing.”
NSA Director, Gen. Keith Alexander, *tells the New York Times* that the agency protects privacy:

“We followed the law, we follow our policies, we self-report, we identify problems, we fix them,” he said. “And I think we do a great job, and we do, I think, more to protect people’s civil liberties and privacy than they’ll ever know.”
The “talking to a foreigner” exception:

[T]he privacy interests of U.S. persons in international communications are significantly diminished when those communications have been transmitted to or obtained from non-U.S. persons located outside the United States. [Marshall et al. 2014, 26]

It’s a version of the “voluntary disclosure” doctrine – when you share information with a third party, it’s no longer private.
Foreign Intelligence Surveillance Act (FISA)

§ 702b

(b) Limitations
   An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States

[emphasis added]

Compare Justice Brandeis’ warning in his *Olmstead* dissent:

the tapping of one man’s telephone line involves the tapping of the telephone of every other person whom he may call or who may call him.
UK’s Regulation of Investigatory Powers Act (RIPA, 2000) – Charles Farr, Director General of the Office for Security and Counter Terrorism at the Home Office, testified that inadvertent intrusions on “domestic” communications are “insignificant”:

individual analysts may have to listen to or look at on screen whatever comes before them, be it relevant to an investigation or not. They are experienced and trained to identify quickly and isolate items of legitimate intelligence interest and to deal with them appropriately;

material which is of no intelligence interest is very quickly passed over, as often as not without being read or listened to. In many systems it is immediately marked for deletion. The deletion will then very soon happen, in many systems automatically;

*meanwhile the analyst, being only human and having a job to do, will have forgotten (if he or she ever took it in) what the irrelevant communication contained.* I have sat next to analysts and heard or seen this happening;

any assessment of the degree of real intrusion should appreciate that this is what inevitably happens on the ground. The active intrusion is insignificant.” [Farr 2014, 35; emphasis added]
According to Farr, the innocent have nothing to fear from government spying:

I am ... personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant.
Just as governments see surveillance as good for national security, corporate surveillance is “good for business” – it’s capitalism at its best:

“Google’s technologists view . . . their effort as helping us figure out the answer to our needs before we know we have those needs.”

Julia Angwin, 2014.
“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.”

“BIG BROTHER IS WATCHING YOU”

George Orwell, 1984
CCTV portrayed as guaranteeing security in a dangerous world . . . and as a warning to those who are up to no good.
Automatic license plate readers do more than let you pay tolls with your EZ-Pass;

Location-based information like license plate data can be very revealing. By matching your car to a particular time, date and location, and then building a database of that information over time, law enforcement can learn where you work and live, what doctor you go to, which religious services you attend, and who your friends are.

https://www.eff.org/foia/automated-license-plate-readers
Law enforcement agencies treat the ALPR information that they collect as secret because it’s part of an ongoing investigation, even if it’s never linked to a crime; and revealing just what information they collect would invade the public’s privacy:

The mere fact that ALPR data is routinely gathered and may not—initially or ever—be associated with a specific crime is not determinative of its investigative nature.

Members of the public would be justifiably concerned about LAPD releasing information regarding the specific locations of their vehicles on specific dates and times—information acquired and maintained strictly for investigatory purposes—to anyone, given that this information can be used to, for instance, draw inferences about an individual’s driving patterns and past whereabouts. [LAPD 2014, 8]
Corporations like Google and Facebook, which collect massive amounts of data on us, react with anger when the government spies on them.

The Snowden leaks revealed that the NSA had created a fake Facebook page which it used to plant surveillance software on the computers of thousands of visitors lured to the site.

Facebook’s Mark Zuckerberg, who had claimed in 2010 that evolving social norms had led to the death of privacy, actually telephoned Pres. Obama directly to protest this government invasion of the privacy of his corporation (Cade 2014).
Thomas L. Friedman, writing in the *New York Times* (2014), on the death of privacy in the digital age:

> [E]veryone with a cellphone camera is paparazzi, everyone with access to Twitter and a cellphone voice recorder is a reporter and everyone who can upload video on YouTube is a filmmaker, everyone else is a public figure — and fair game.
The view from GoogleGlass:
Combined with facial recognition software, it’s not just images that get uploaded, it’s identities:

NameTag checks the picture against social media data. Facebook alone has over 3 billion indexed images.

What are the privacy implications of that?

The same developer markets CreepShield, which checks a facial image against a database of registered sex offenders.
The e-reader over your shoulder:

CCTV may monitor our comings and goings from the outside, but e-readers have spyware that actually looks inside our heads. Our ebooks read us as we are reading them.

They track what we read, how fast we read, where we pause, what we highlight, what words we look up in the built-in dictionary.

That information translates into marketing decisions – but it also provides “feedback” to authors.

Writing books will be like producing TV shows, testing everything with focus group before releasing it to the public.

Librarians regularly go to jail to avoid divulging patron borrowing information, but Amazon and Apple will routinely obey law enforcement requests for the reading data they collect about you.
It says “buy now with 1-Click, but you’re really renting, not owning:

You may not sell, rent, lease, distribute, broadcast, sublicense, or otherwise assign any rights to the Kindle Content or any portion of it to any third party.

Amazon Kindle Terms of Service Agreement, 2012

Users who violate the agreement may have their access to Kindle blocked and their content confiscated, with no refund of any fees paid.
The Right to Be Forgotten

Costeja González sued Google in the European Court of Justice to have this 12 year old link to his debt problems removed.

He won “the right to be forgotten,” which is about to be enshrined in EU law.
the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person . . . even, as the case may be, when its publication in itself on those pages is lawful.

[European Court of Justice 2014, ruling par. 3;]
Website owners whose links have been removed now receive this notice from Google.
The European Commission is proposing a new data regulation law that will guarantee “the right to be forgotten and to erasure.”

According to an EC fact sheet,

The right to get your data erased is not absolute and has clear limits. . . . A case-by-case assessment will be needed. *Neither the right to the protection of personal data nor the right to freedom of expression are absolute rights.* A fair balance should be sought between the legitimate interest of internet users and the person’s fundamental rights. Freedom of expression carries with it responsibilities and has limits both in the online and offline world. . . .

The right to be forgotten is certainly not about making prominent people less prominent or making criminals less criminal.

[European Commission 2014, emphasis added]

Is this privacy protection or censorship?
What about the provision to judge requests on a case-by-case basis?
And what about Costeja González and his right to be forgotten?

The links remain on Google searches of the name Mario Costeja González that are done outside of Europe:
And for European searches, Google erased the link to the newspaper notice of Costeja González’ debt auction.

But the links to his ECJ lawsuit remain, and many of them mention his debt problems.

His “right to be forgotten” lawsuit ensures that Costeja González will be remembered both as a debtor and as the man who sued Google and won.