Robert Ellis Smith
Attorney and Publisher,
Privacy Journal Newsletter

www.privacyjournal.net
Numbers dialed to and from a phone are not entitled to as much privacy protection as the content of the conversation. Therefore no prior court approval is necessary.

U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735 (1979)
In 2014 the opposite is true. Most cell conversations are not probative, not sensitive, not revealing.

But the numbers dialed to us and from us show our associations and our patterns. (You can determine that a person called an abortion or AIDS clinic from the numbers dialed but less so from the content of the words spoken.)
NSA recognizes this. It collects “megadata” on all Americans precisely to establish their patterns, possible associations with terrorist groups. It does not regard suspicion as a predicate to collect the data.
Poll:

Do you store information on the whereabouts of a student or employee?

- Yes
- No
- Not sure
“The main thrust of the government’s argument here is that under Smith, no one has an expectation of privacy, let alone a reasonable one, in the telephony metadata that telecom companies hold as business records.

To say the least, “whether the installation and use of a pen register constitutes a ‘search’ within the meaning of the Fourth Amendment under the circumstances addressed and contemplated in that case is a far cry from the issue in this case.”

“When do . . . the evolutions in the government’s surveillance capabilities, citizens’ phone habits, and the relationship between the NSA and telecom companies become so thoroughly unlike those considered by the Supreme Court 34 years ago that a precedent like Smith simply does not apply? The answer is now.”

Klayman v. Obama
Poll:

Which is the most sensitive in your environment?

- Academic record
- Student disciplinary record
- Location of a person in real time
- Work history
Cell phones have also morphed into multi-purpose devices. They are now maps and music players. They are cameras. They are even lighters that people hold up at rock concerts.

*Klayman v. Obama*
Poll:

Are you aware of the security-breach notification requirement in your state?

- Yes
- No
- Not sure
Poll:
What is the federal breach-notification requirement?
“The myth: This idea that as long as the NSA is ‘only collecting metadata’ then we can live with that level of intrusion, but when it comes to listening to people’s cell phone calls or reading their emails, that’s when genuine outrage is warranted.”

“This is probably the single greatest misconception in the reporting that we’ve been doing.”

Glenn Greenwald, formerly of The Guardian, Dec. 18, 2013
“If you talk to surveillance experts, what you will hear around the world is that collection of ‘metadata’ is not as invasive as the interception of the content of conversations. But collection of metadata is now more invasive than interception of content. And it isn’t just surveillance experts who think that way; it’s the NSA itself. Throughout these documents appears the recognition that collecting metadata is the supreme priority.”

Glenn Greenwald
“It’s difficult to understand that in the abstract, but it’s easy to understand it when concrete examples are used. If you can imagine a woman who decides that she wants to get an abortion, if you’re listening in on her phone call, what you will hear is her calling the clinic; the clinic will answer with a generic-sounding name, like ‘East Side Clinic’ or something like that; you will hear the woman whom you decided to target for surveillance ask for an appointment, and then hang up the phone. As an investigator, you’ll have no idea why she called, or even what kind of clinic she called, or what the purpose was.”

Glenn Greenwald
Poll:

In the past 5 years, have you:

- Experienced a serious breach?
- Had to report a breach?
- Not sure
Sensitivity

“But if you’re collecting her metadata [numbers dialed to and from her phone, location of the nearest cell tower], you will see the phone number that she called; you will then be able to identify it as an abortion clinic; you will know how many times she called that clinic; and you will have exactly the information that you wouldn’t get if you were simply listening to her phone call.

“The same is true with somebody who has HIV and calls a doctor.

“The same with somebody who calls a suicide hotline or a drug addiction clinic, or somebody who is speaking with someone who is not his or her spouse late at night.”

Glenn Greenwald
Sophisticated Analysis

“There are now increasingly sophisticated tools for analyzing metadata when it’s collected *en masse*, to be able to understand not only whom your targets are speaking to, but whom those people are speaking to, and then who those people are calling, and to develop a very comprehensive picture of the network of associations and friends of various individuals.”

“You have a very invasive understanding of the private behavior, the private associations, the private thoughts of the people whom you place under surveillance.”

Glenn Greenwald
The new trend of this decade: Data about our whereabouts is far more sensitive than data about ourselves – including medical, financial, school, credit, employment data. ATMs, GPS, cell towers, employee and student IDs.

Data about our calling patterns is far more sensitive than the content of our calls.
The principles of fair information practice do not necessarily fit the new reality.

Organizations establishing privacy policies should incorporate the elements of the widely accepted *Code of Fair Information Practice*:
CODE OF FAIR INFORMATION PRACTICE

• The existence of all data systems with personal information in them should be publicly disclosed, and the purpose for which information is gathered about people should be disclosed. This is the principle of openness or transparency.

• There must be a way for an individual to find out what information about him or her is in a record and how it is used.
There must be a way for an individual to prevent information about him or her that was obtained for one purpose (which was stated when the information was gathered) from being used or made available, either within the organization or outside, for a purpose that is incompatible with the original purpose, without getting the consent of the individual. This is the principle of secondary use.

There must be a way for an individual to correct or amend a record that contains information that is identifiable to him or her.
THE NEW REALITY

Location, location, location

Threats to our privacy come in intrusions into our whereabouts:

- ATMs, GPS, cell-phone towers, video surveillance on highways and downtown
- ID cards and RFID tags for entry into buildings and workplaces
- StreetView (now inside large buildings and parks), electronic entry systems on campus
RESOURCES

Current laws on privacy protection:

- *Compilation of State and Federal Privacy Laws 2013*, hard copy from *Privacy Journal* or Amazon ($35), electronic from *Privacy Journal* ($26.50) or Kindle.

History of privacy in America:

- *Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, including Social Security numbers, credit and medical records, eavesdropping, and the torts of invasion of privacy, hard copy from *Privacy Journal* or Amazon ($17.50), electronic from *Privacy Journal* ($17.50) or Kindle.
RESOURCES

Higher education:


Security-breach notification:

• “Who’s Protected by State Breach-Notification Laws?” *Privacy Journal*, January 2014, free from *Privacy Journal*, [orders@privacyjournal.net](mailto:orders@privacyjournal.net), also published by [www.extractsystems.com](http://www.extractsystems.com)
RESOURCES

Use of Facebook and Google by Admissions:


MONTHLY NEWSLETTER:

• *Privacy Journal*, hard copy or electronic, $125 a year

• Sample from [orders@privacyjournal.net](mailto:orders@privacyjournal.net).

www.privacyjournal.net