Question 1....

Describe the heart of the chapter in two (or three) words

Question 2...

The authors’ analogy was to “footprints” and “fingerprints”...

What's the difference?

Can you give a few examples of each?
Digital Tracks Everywhere... examples

Footprints ("data trails we leave intentionally")
- Pictures posted to social networking web sites
- Tax records, phone bills, financial transactions, ... 
- Customer loyalty cards
- Car tracking - GPS in rental cars, data recorders in all cars, toll speed-pass

Fingerprints ("data trails of which we are unaware or unconscious")
- Metadata in pictures (GPS, camera serial number, etc.)
- Printouts from color laser printers
- Web browsing or search history
- An additional one: POSTNET printed on US mail for routing

Views toward privacy

Scott McNealy, (CEO of Sun at the time):
"You have zero privacy anyway. Get over it."

Are there generational differences? (Student comment)
Does that come from age, or culture change?

Privacy drastically different from 50 years ago.
How did this happen?
How do you boil a frog?
(This anecdote apparently isn't true... just so you know)

What privacy do you give up in "I Agree" buttons?

What about at UNCG? By using UNCG resources (Blackboard, E-mail, etc.):

No University employee, student or any other user shall have any expectation of privacy in the material or information sent or received using any portion of the University information system infrastructure, information systems, or systems containing University information assets. For security, legal, investigative, policy compliance, quality of service, and infrastructure maintenance purposes, authorized employees within ITS, and those University employees outside ITS with responsibilities necessitating access, may monitor information system and infrastructure activity and/or content, in the course of discharging their duties.

Source: UNCG Policy on "Acceptable Use of Computing and Electronic Resources"
http://policy.uncg.edu/acceptable_use/
From student comments

Attitude toward privacy: "I would think that would help the crime rate go down.

- More than one student had an "if you have nothing to hide..." attitude
- Crime rates would also go down if police did monthly home inspections of all people. And surely, if you have nothing to hide...

On leaving tracks: "Leaving electronic fingerprints, like im doing with this assignment."

- Do you know what happens to your work after the course is over?
- [Link](http://its.unbc.edu/Records_Management/General_Schedule/)
- (Second point: "im???? Really?")

Several students mentioned SOPA/PIPA/ACTA bills - less of a privacy issue than balancing freedom vs intellectual property - will get to later!

Several students interested in RFID

Electronic tags that can easily be made unique (unique serial numbers)
- Great for tracking!

Extremely low cost

Passive tags don't require a battery

Shipping containers, library books, individual products,
...

In clothing tags...

Source: "RFID Journal", March 12, 2003
In Passports...

Bad guys could read RFID passports at 217 feet, maybe a lot more.

By Timextor, Network World
July 29, 2015 10:22 PM

LAB VIGILANTE — Radio frequency ID tags embedded in U.S. passports can be read hundreds of feet away, potentially making it exceedingly easy to jock American tourists out of their credit for RFID朐s by a demonstration of the Black Hat 2015 showed.

10 cutting-edge new gadgets

Using off-the-shelf gear bought in stores cost roughly $100, investigator Chris Paget put together a system that he says can read the tags at 217 feet but no longer than 100 feet if weather conditions could result in an 800-foot read.

He says he is willing to give a whirl during the Black Hat conference if someone can get the device to a sensitivity.

The same RFID chips are used in Canadian passports and in New York state driver's licenses, he says. They are also used for inventory control at Walmart.