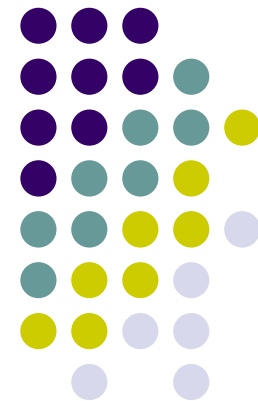


Perspectives on Privacy

The Technological View

Carlisle Adams
School of Information Technology and Engineering
University of Ottawa



Generalizing Tessling...



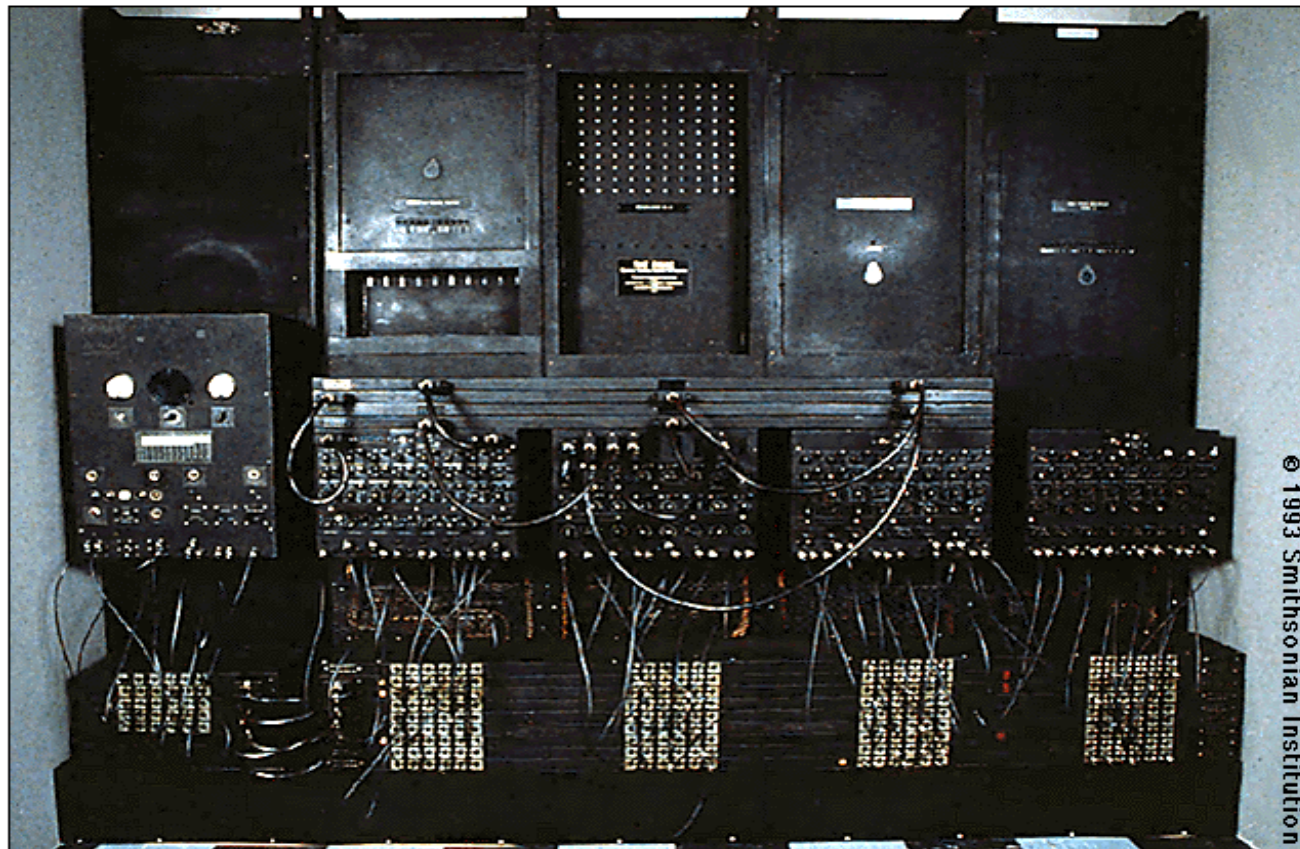
- The Tessling case has to do with heat emanating from a house
 - We can think of this as a flow of data from inside the house to outside the house
 - “**Communication**” of data from a source/sender (inside) to a destination/receiver (outside)
 - *The question is: how does privacy relate to this?*
- We approach this from the perspective of communications technology (e.g., the Internet) and its relationship to privacy

Roadmap

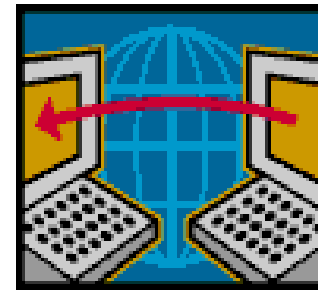
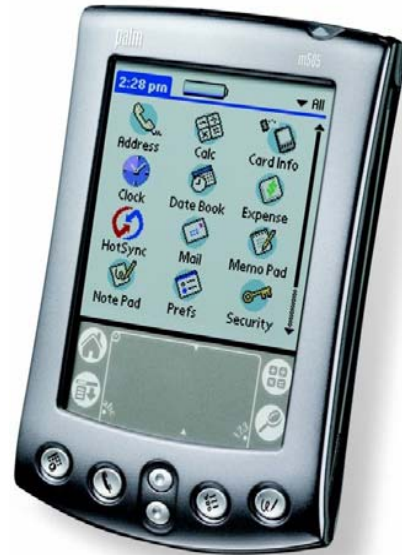


- Thinking through the process
 - Communication technology
- Putting the pieces together
 - Implications of successful communication
- The path forward
 - Techniques for achieving privacy
- Conclusions

Early Days of Computing



Slightly more recently...





The world of computing and communications has changed drastically over 50 years...

...but in the fundamentals, perhaps not so much

Consider two people, Alice and Bob, that wish to communicate

Thinking through the process



Hi Bob!

Alice

Bob



Thinking through the process



Hi Bob!

Alice

Bob

H

H

Thinking through the process



Hi Bob!

Alice

Bob

i

Hi

Thinking through the process



Hi Bob!

Alice

B

Bob

Hi B

Thinking through the process



Hi Bob!

Alice

Bob

o

Hi Bo

Thinking through the process



Hi Bob!

Alice

b

Bob

Hi Bob

Thinking through the process



Hi Bob!

Alice

Bob

!

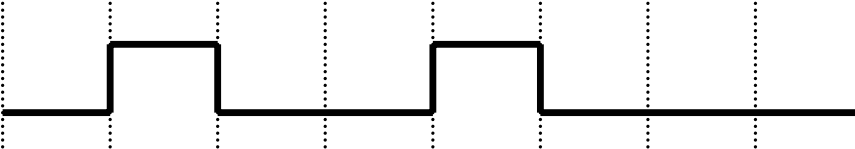
Hi Bob!

- How does Alice send “H” (“i”, “B”, “o”, “b”, “!”)?
 - “H” is encoded (universally) as “01001000”
 - “i” is encoded as “01101001”, and so on...
- So, how does Alice send “0” and “1”?

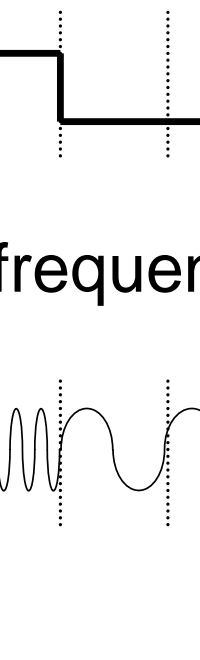


Thinking through the process (cont'd)

- One method: turn wire voltage on and off

● “01001000” = 

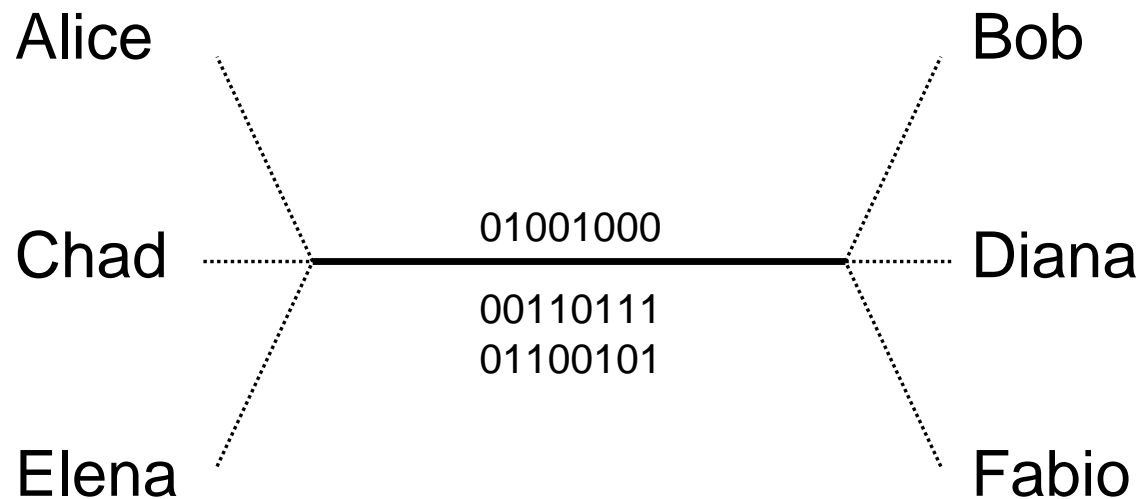
- Another method: use different frequencies

● “01001000” = 



Why is this important?

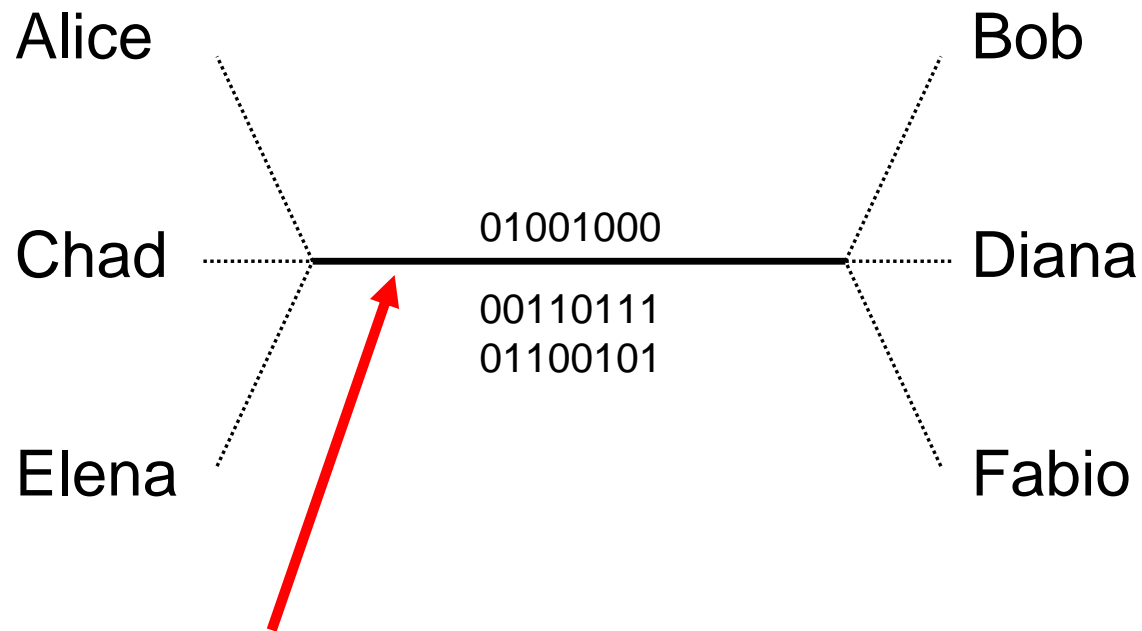
- Alice and Bob are not alone in the world



- Shared link (multiplexing): on/off voltage requires taking turns, but many frequencies can be sent at once



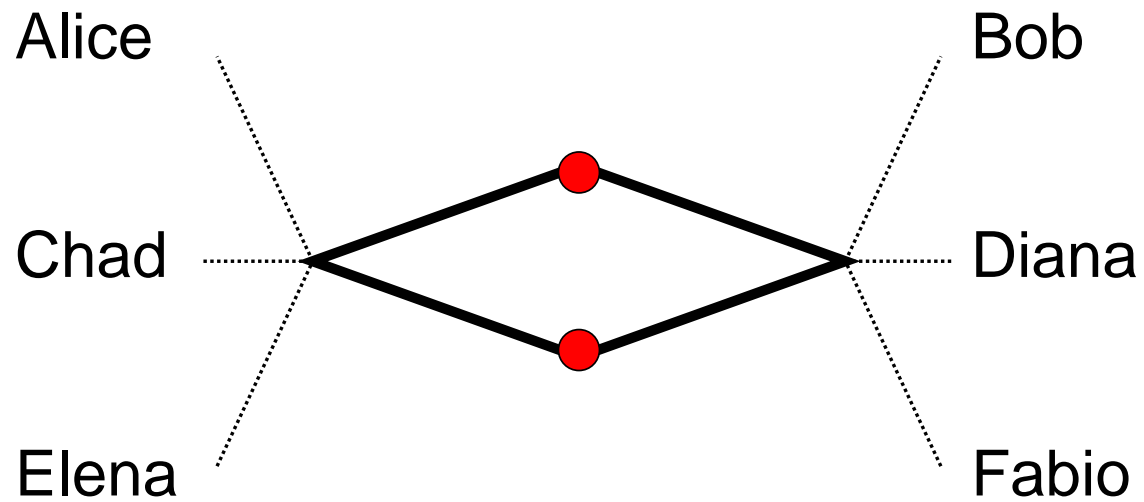
Another important feature



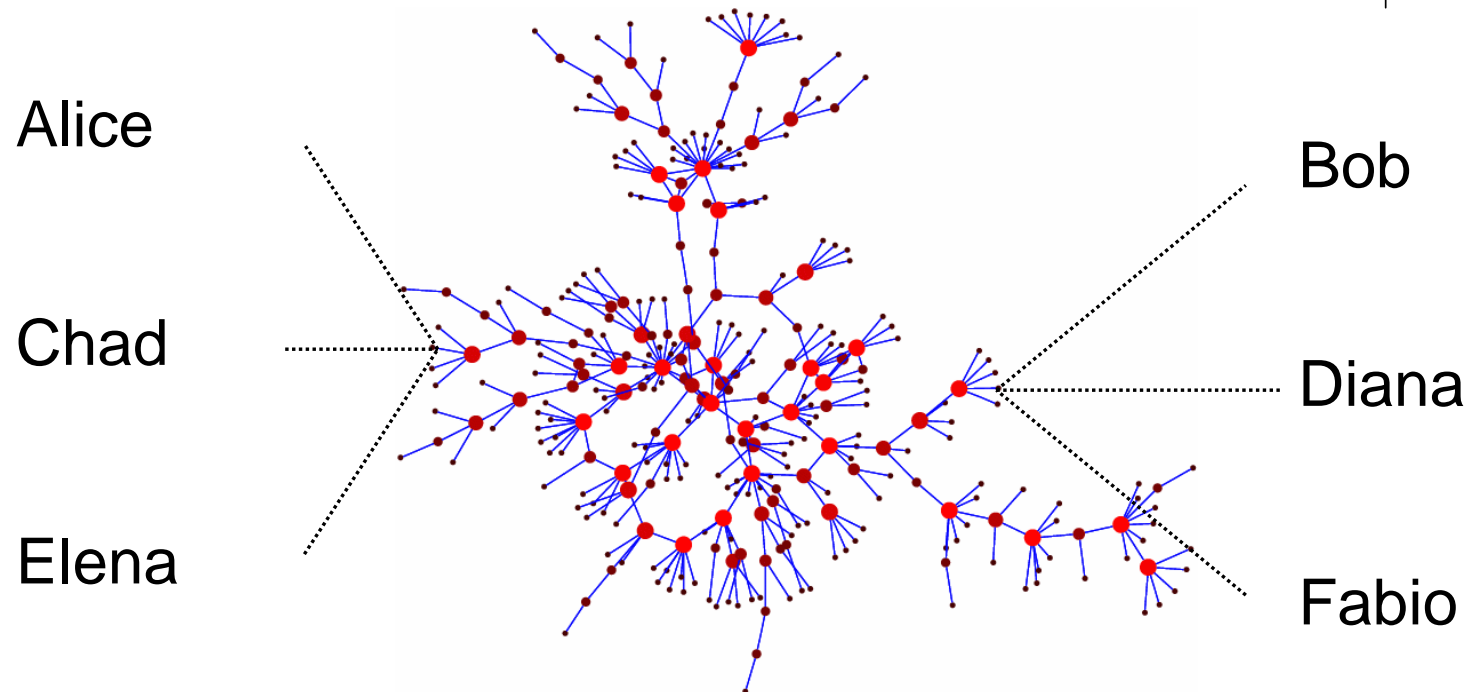
What if this link dies (gets broken; stops working)?

- Lots of unhappy people...

Solution: alternate routes



Slightly more realistic picture...



- Many, many ways to get from sender to receiver (high connectivity)



Thinking through the process (cont'd)

- What do we want from a communications network?
 - Efficiency and reliability
- How is this achieved?
 - Multiplexing and connectivity

Assign traffic to
time slots or
frequencies

Assign routing
information to
data packets

Putting the pieces together



- Multiplexing and connectivity require identification and addressing information (on every packet sent)

Oh-oh...

The very things that make a communications network “good” (e.g., efficiency and reliability) are the things that reduce privacy to zero.

UNreasonable expectation of privacy!

(over Internet, cell phones, IM links, LANs, etc.)

But...



- Isn't my data "lost in the crowd"?
 - Fibre optic line has a capacity of over 40 Gb/s
 - Roughly equivalent to every man, woman, and child on planet Earth saying "Hi there!" simultaneously over a 10-second period
- Well, no.
 - The addressing information on each packet (along with highly sophisticated searching and filtering algorithms) make finding a message, and tying it to Alice, quite feasible [after all, it's communications!]

Roadmap



- Thinking through the process
 - Communication technology
- Putting the pieces together
 - Implications of successful communication
- The path forward
 - Techniques for achieving privacy
- Conclusions

The Path Forward



- Let's be precise about where our thinking has led us
 - We've said that a "good" communication technology is engineered for efficiency and reliability, and that these features run counter to privacy
 - We have NOT said that that there can be no privacy in digital communications
 - Privacy is not an inherent characteristic of the technology, but it can be added to (imposed upon) the technology, for the benefit of users

Techniques for Achieving Privacy



- Many techniques exist for enhancing privacy on the Internet and other comm's networks
 - These may be classified, at a first level, according to **how** personal data is protected
 - technological mechanisms (those that exclusively or primarily use computers and software to implement privacy), or
 - societal mechanisms (those that exclusively or primarily use human means to implement privacy)



Techniques for Achieving Privacy (cont'd)

- Within these broad branches, the techniques may be further sub-divided according to a number of other classifiers
 - **Who** is holding the data (the subject, or a 3rd party)?
 - **What** is the data (real-time action, or static attribute)?
 - **When** is the data protected (as it is released to intended targets, or as it is acquired by unintended recipients)?
 - **Where** is protection applied (on identity, on action/attribute, or on both)?

Classification for Privacy Techniques



- Existing Privacy Enhancing Technologies (PETs) fit well within the proposed classification
 - MIX networks, anonymizers, encryption mechanisms, de-identification, and so on
- On the societal side, the legal infrastructure offers some solutions in various branches of the proposed classification
 - privacy laws, gov't- or sector-imposed privacy guidelines, contractual obligations for personal data, and so on
- Such a classification allows for more meaningful comparison and contrast of techniques, and highlights deficiencies that need to be addressed as well as techniques that are truly complementary



Roadmap

- Thinking through the process
 - Communication technology
- Putting the pieces together
 - Implications of successful communication
- The path forward
 - Techniques for achieving privacy
- **Conclusions**

Conclusions



- A good communications path does not inherently possess privacy characteristics (conflicting goals!)
 - True of digital networks (wired & wireless; pt2pt & broadcast)
 - May also be true of heat passing through house walls...
 - (No destination address, but what about source address?)
- However, privacy can be imposed on any given communications path through technological and/or societal mechanisms (e.g., legal, sociological, psychological, and philosophical means)
- *Therefore, it is rational to conclude that privacy does exist (or can exist), even if there is no technical basis for a “reasonable expectation of privacy”*