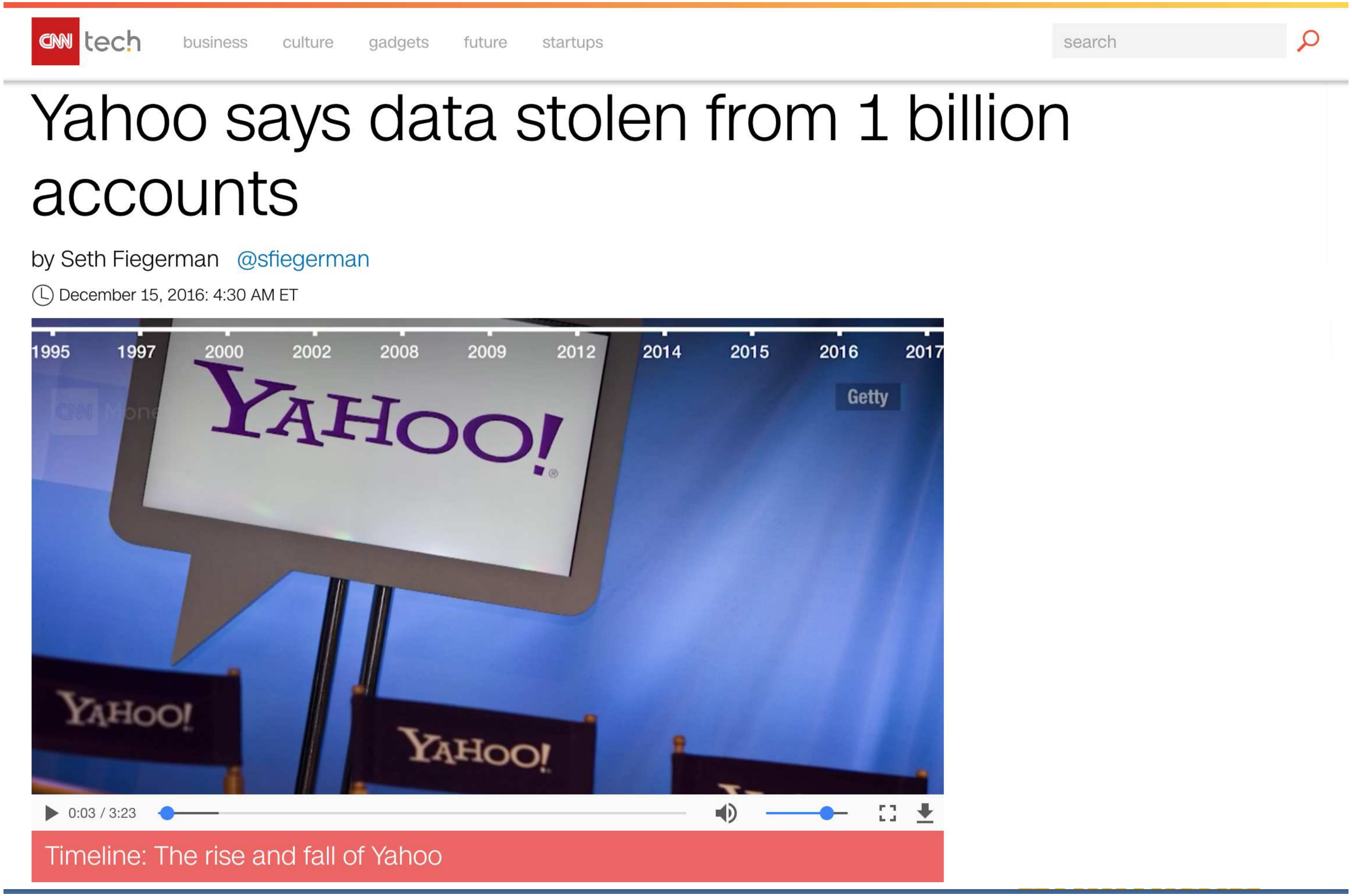
Lecture 02 – Ethics

Stephen Checkoway

CS 343 – Fall 2020

Adapted from Michael Bailey’s ECE 422

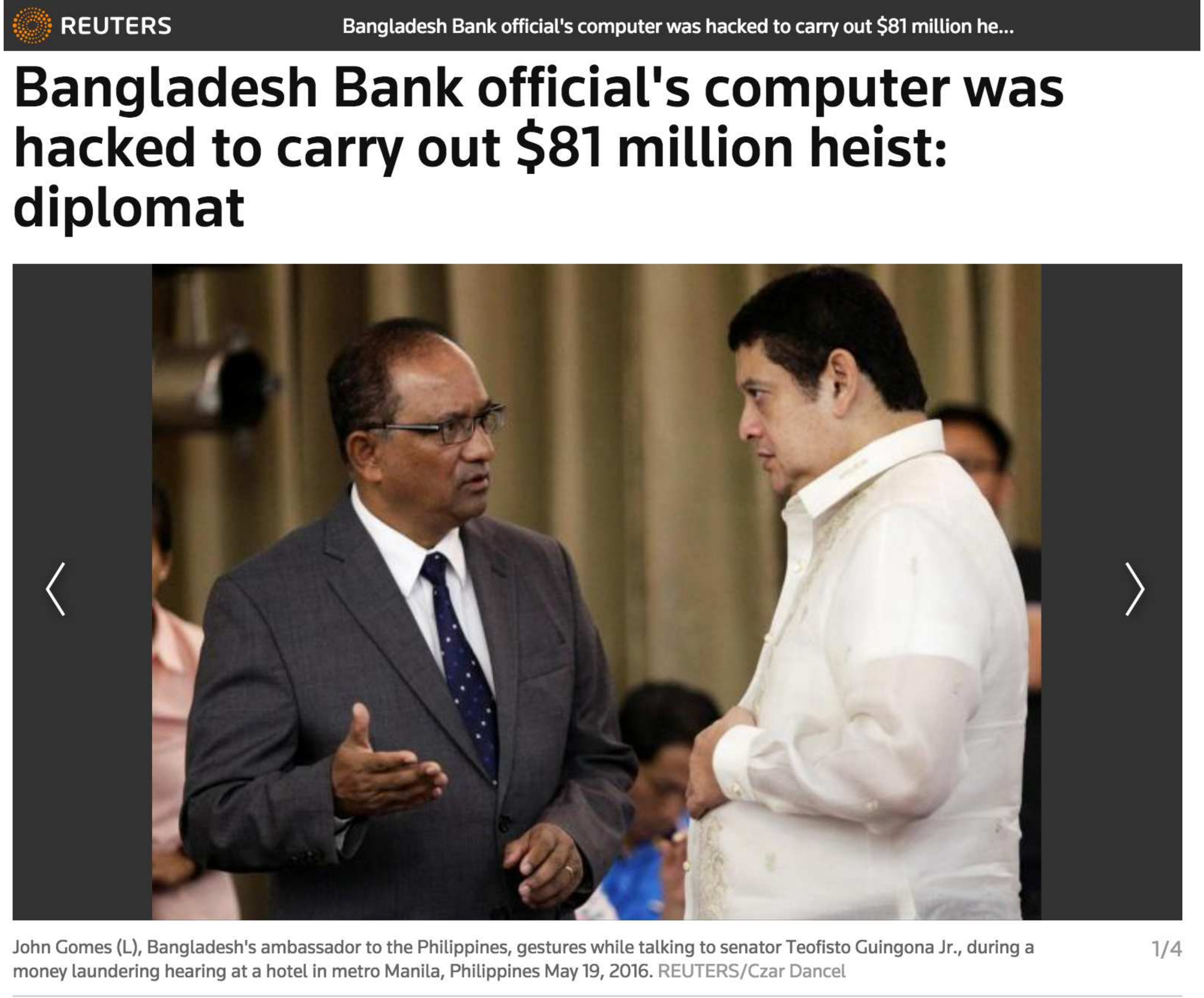


Yahoo says data stolen from 1 billion accounts

by Seth Fiegerman @sfiegerman

December 15, 2016: 4:30 AM ET

Timeline: The rise and fall of Yahoo

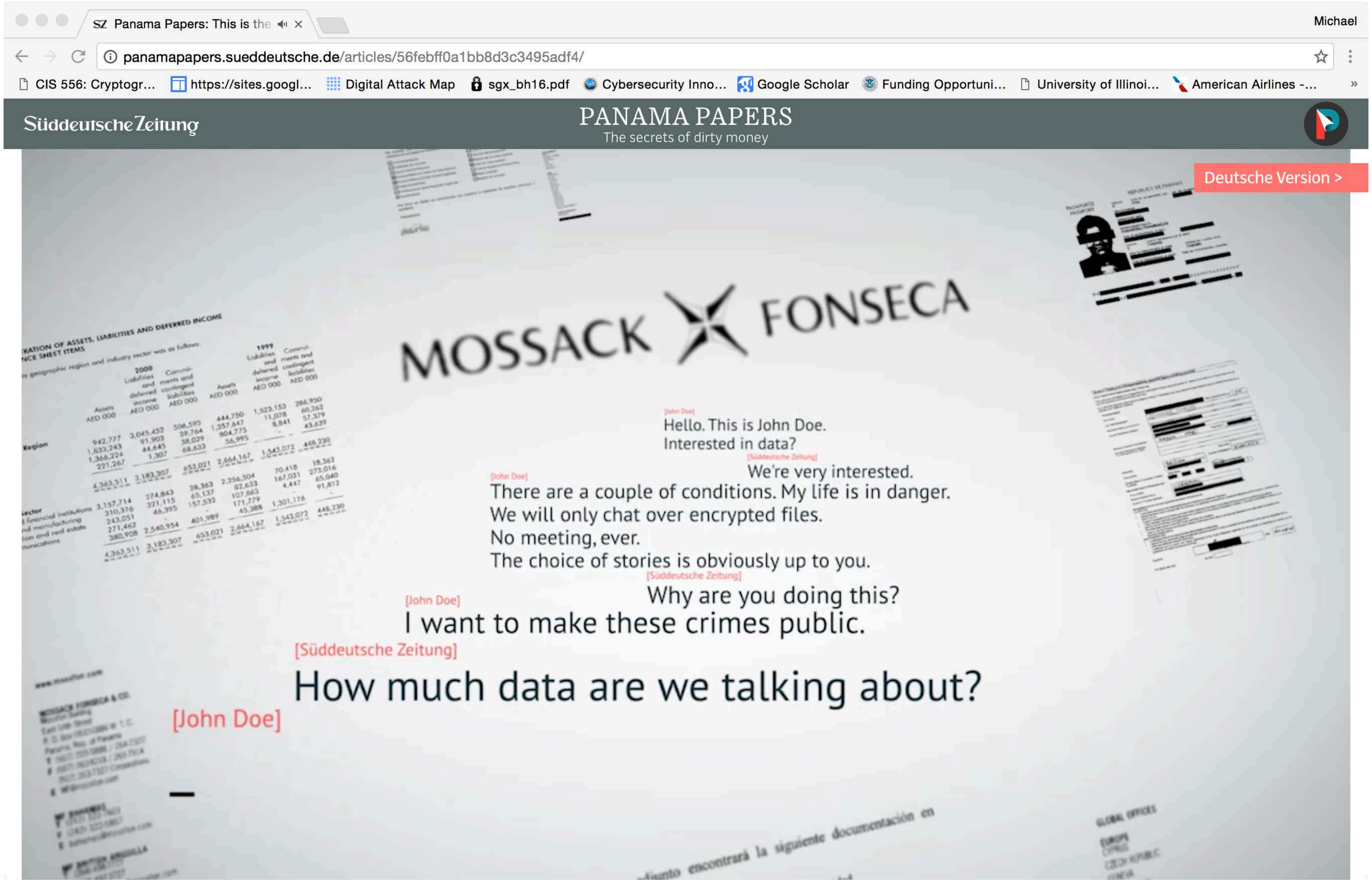


REUTERS Bangladesh Bank official's computer was hacked to carry out $81 million he...

Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat

John Gomes (L), Bangladesh's ambassador to the Philippines, gestures while talking to senator Teofisto Guingona Jr., during a money laundering hearing at a hotel in metro Manila, Philippines May 19, 2016. REUTERS/Czar Dancel

1/4



[John Doe]
Hello. This is John Doe.
Interested in data?

[Süddeutsche Zeitung]
We're very interested.

[John Doe]
There are a couple of conditions. My life is in danger.
We will only chat over encrypted files.
No meeting, ever.
The choice of stories is obviously up to you.

[Süddeutsche Zeitung]
Why are you doing this?

[John Doe]
I want to make these crimes public.

[Süddeutsche Zeitung]
How much data are we talking about?

[John Doe]

Gary Cameron / Reuters

Did Putin Direct Russian Hacking? And Other Big Questions

Thank goodness for security experts

Security "Research" to the Rescue!

- Researchers want to help, to benefit the *internet community*
- …but oh, the temptations!

  First to publish; do something new; show how 1337 you are; fight for funding; ends justify the means

- …and the conflicts

  Affecting other research; impacting LE investigations; thwarting mitigation efforts; protecting rights; helping the bad guys; less risky (and less sexy) options?

What are ethics?

- “The field of ethics (or moral philosophy) involves systematizing, defending, and recommending concepts of right and wrong behavior.”
- Normative ethics, is concerned with developing a set of morals or guiding principles intended to influence the conduct of individuals and groups within a population (i.e., a profession, a religion, or society at large).
    - Consequentialism: Consequences are the most important consideration
    - Deontology (duty-based ethics): Following rules is most important
    - Virtue ethics: An individual’s character is more important than either actions or consequences

Philosophy 101-level ethics problem

- Situation: You’ve been captured along with 10 other people and your captors give you a choice: Shoot one of the 10 people yourself and everyone else lives or shoot no one and your captors will kill all 10.
- Deontological (duty-based) ethics may have a rule, “do not kill” so the ethical thing to do is kill no one (but then 10 people die)
- Consequentialism may dictate that one dead person is a better outcome than 10 dead people so the ethical thing to do is to shoot

Computer Ethics

"A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with **new capabilities** and these in turn give us **new choices** for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine **what we should do** in such cases, i.e., to formulate policies to guide our actions."

-Moor

Ethics != Law

- “Law can be defined as a consistent set of universal rules that are widely published, generally accepted, and usually enforced”
- Interrelated but by no means identical (e.g., legal but not ethical, ethical but not legal)
  - Adherence to ethical principles may be required to meet regulatory requirements surrounding academic research
  - A law may illuminate the line between beneficial acts and harmful ones.
  - If the computer security research community develops ethical principals and standards that are acceptable to the profession and integrates those as standard practice, it makes it easier for legislatures and courts to effectively perform their functions.

IANAL

- Computer Fraud and Abuse Act (CFAA)
  - "it is illegal to intentionally access a computer without authorization or in excess of authorization and thereby obtaining information from any protecting computer."
- Digital Millennium Copyright Act (DMCA)
  - “No person shall circumvent a technological measure that effectively controls access to [a work protected by copyright law]”
- Electronic Communications Privacy Act (ECPA)
  - Wiretap Act — Illegal to intercept/disclose/use contents of wire/oral/electronic communication using a device
  - Pen Register Statute (Part of USA PATRIOT Act) — Makes forms of internet surveillance illegal w/o court order
  - Stored Communications Act — criminal penalties for accessing stored communications without authorization
- State and Local Laws
  - Ohio; Chapter 2913 of Ohio Revised Code
- Computers and networks may carry data for a variety of institutions such as hospitals, libraries, universities, and K-12 organizations
  - Family Educational Right to Privacy Act (FERPA)
  - Federal Standards for Privacy of Individually Identifiable Health Information (implements the privacy requirements HIPAA)

Contracts and Policies

- End User License Agreements (EULA)
  - Do not criticize this product publicly
  - Using this product means you will be monitored
  - Do not reverse-engineer this product
  - We are not responsible if this product messes up your computer
- Organizational Policies

Oberlin College Policy Documents

- Acceptable Use Policy
  https://www.oberlin.edu/cit/policies/acceptable-use-policy
- Network Policy
  https://www.oberlin.edu/cit/policies/network-policy

Existing Ethics Standards

- 1947 Nuremberg Code
- Helsinki Declaration 1964
- The IEEE, ACM, etc: Codes of Ethics
- The Belmont Report, the National Research Act, and Institutional Review Boards (IRB)
  - 45 CFR 46
- “Rules of Engagement”
  - The Law of Armed Conflict
  - Dittrich/Himma: Active Response Continuum
- Other Organizational Codes (Universities, Corporations, etc.)

IRB and the Belmont report

- The primary goal of the Institutional Review Board (IRB) is to assure that, in research involving human subjects, the rights and welfare of the subjects are adequately protected.
- "Ethical Principles and Guidelines for the Protection of Human Subjects of Research”, United States Department of Health, Education, and Welfare, April 18, 1979 (Belmont Report)
- Respect for persons
  - Individuals should be treated autonomously
  - Informed consent should be freely given
- Beneficence
  - Do no harm
  - Maximize possible benefits/minimize risks
- Distributive Justice
  - Equitable selection of research subjects

Professional Ethical Codes

- IEEE Code of Ethics (2006)
  - commits members ”to the highest ethical and professional conduct”. Members agree to avoid conflicts of interest, be honest, engage in responsible decision making, accept criticism of work, etc
- ACM Code of Ethics and Professional conduct (1992)
  - “contribute to society and human well-being”, “avoid harm to others”, along with six other principles (e.g., don’t discriminate, be honest, respect privacy).

Welcome to
NEWBIE
Please drive carefully

Case Study: Botnets

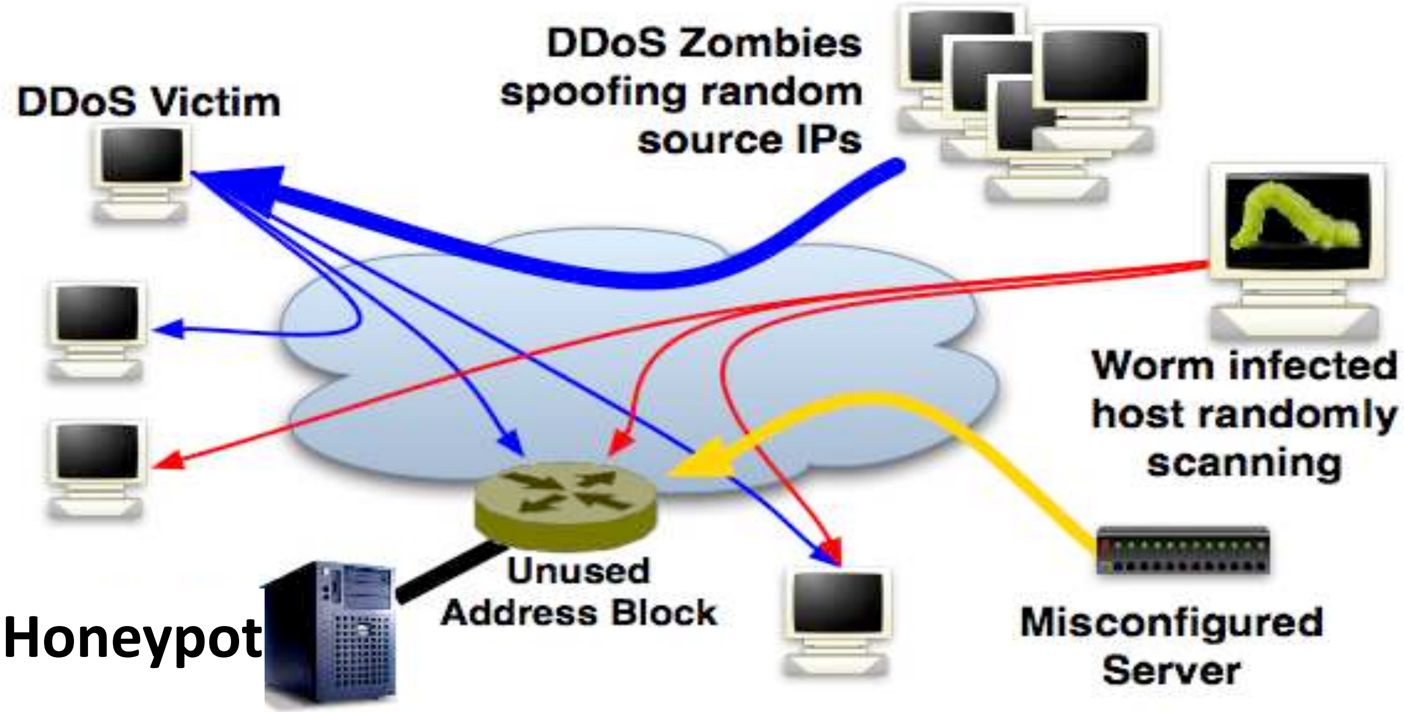
- Botnets, briefly
  - Bots are compromised computers under the control of some 3rd party
  - Collection of bots comprise a botnet
  - Bots communicate with command & control servers which provide instructions, e.g., DDOS a host, send spam, find new machines to infect
  - (Almost) every major security incident today involves botnets

Case Study: Botnets

- A researcher constructs a benign botnet out of compromised routers and uses it to measure the entire Internet; data released publicly and anonymously
- Is this ethical?
- What are the potential issues?

Case Study: Honeypots

- Researchers create a research test beds, connected to the Internet, which enables test bed machines to become infected.


DDoS Victim
DDoS Zombies spoofing random source IPs
Worm infected host randomly scanning
Unused Address Block
Honeypot
Misconfigured Server

Case Study: Honeypots

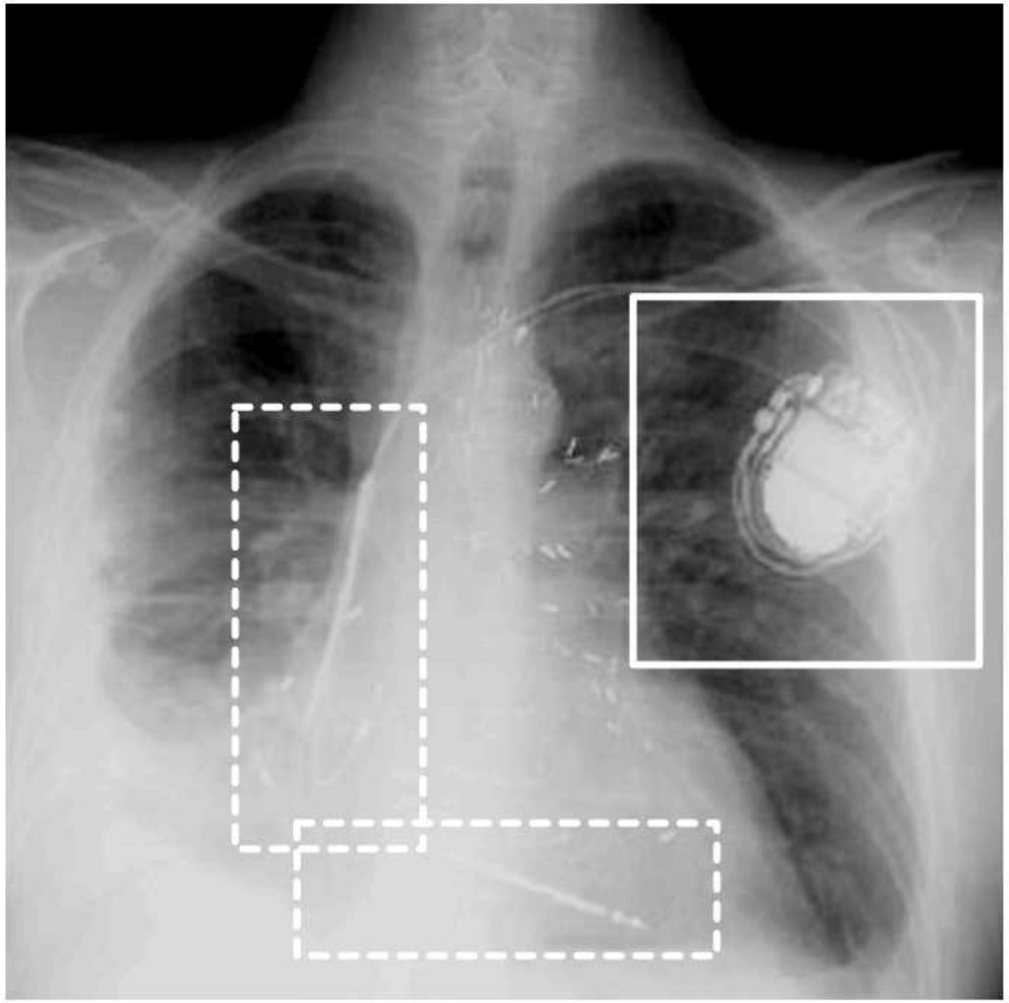
- Why? Capture malware, see exactly what files it creates/modifies/deletes, see its network traffic, find its command and control servers
- Is this ethical?
- What are potential issues?

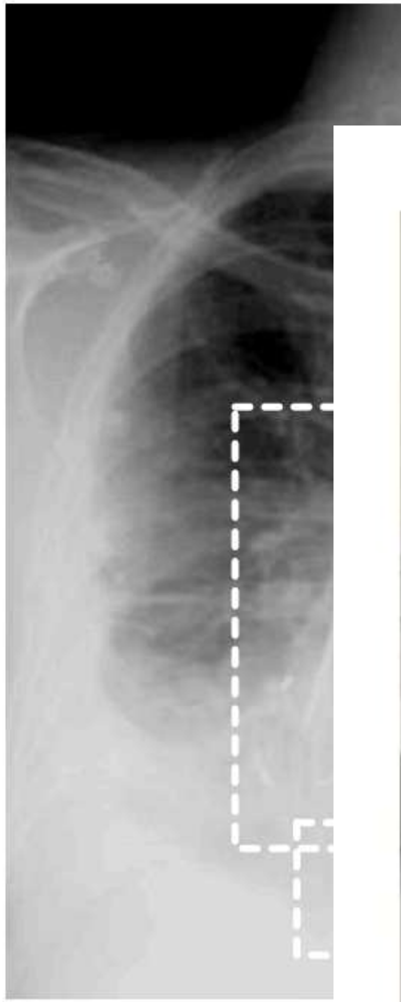
Case Study: Hack back

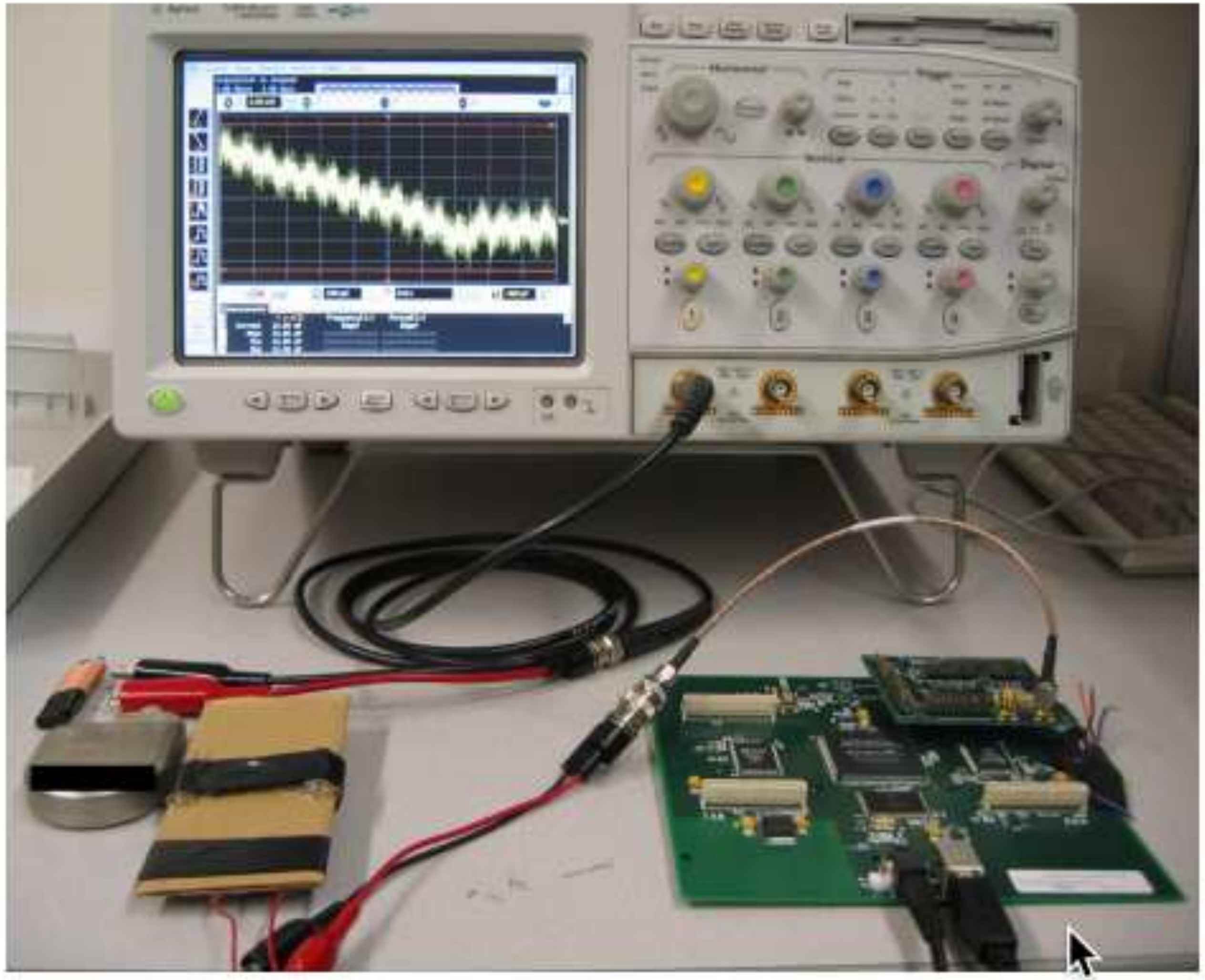
- Organizations get hacked all the time. Sometimes the only (feasible) way to identify the attackers or prevent future attacks is to hack back
- Is this ethical?
- Potential issues?

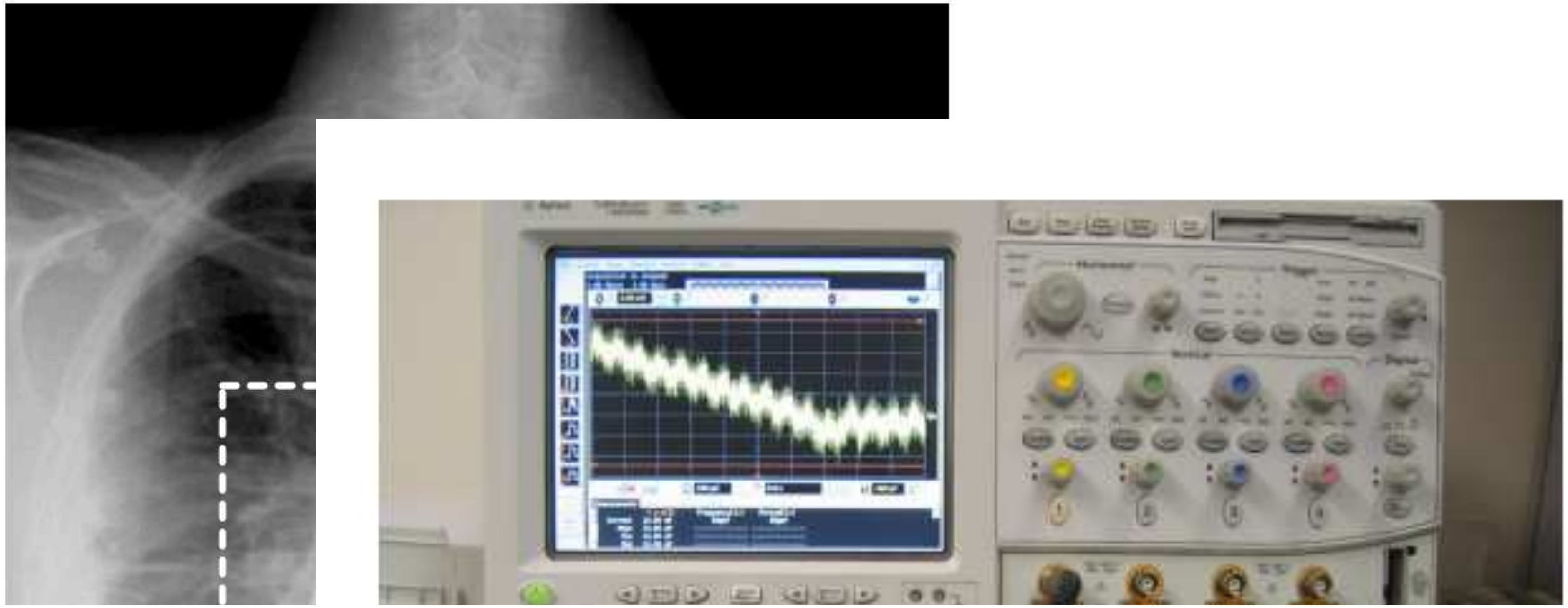
Case Study: Reverse Engineering, Vulnerability Disclosure?

- Researchers reverse engineer a system, discover a vulnerability, and generate a working exploit (attack).
- Lots of debate about how and if one should disclose the vulnerability
  - Full disclosure: go public immediately
  - Give vendor a deadline before disclosure
  - Coordinate disclosure with the vendor
  - (lots of other options)



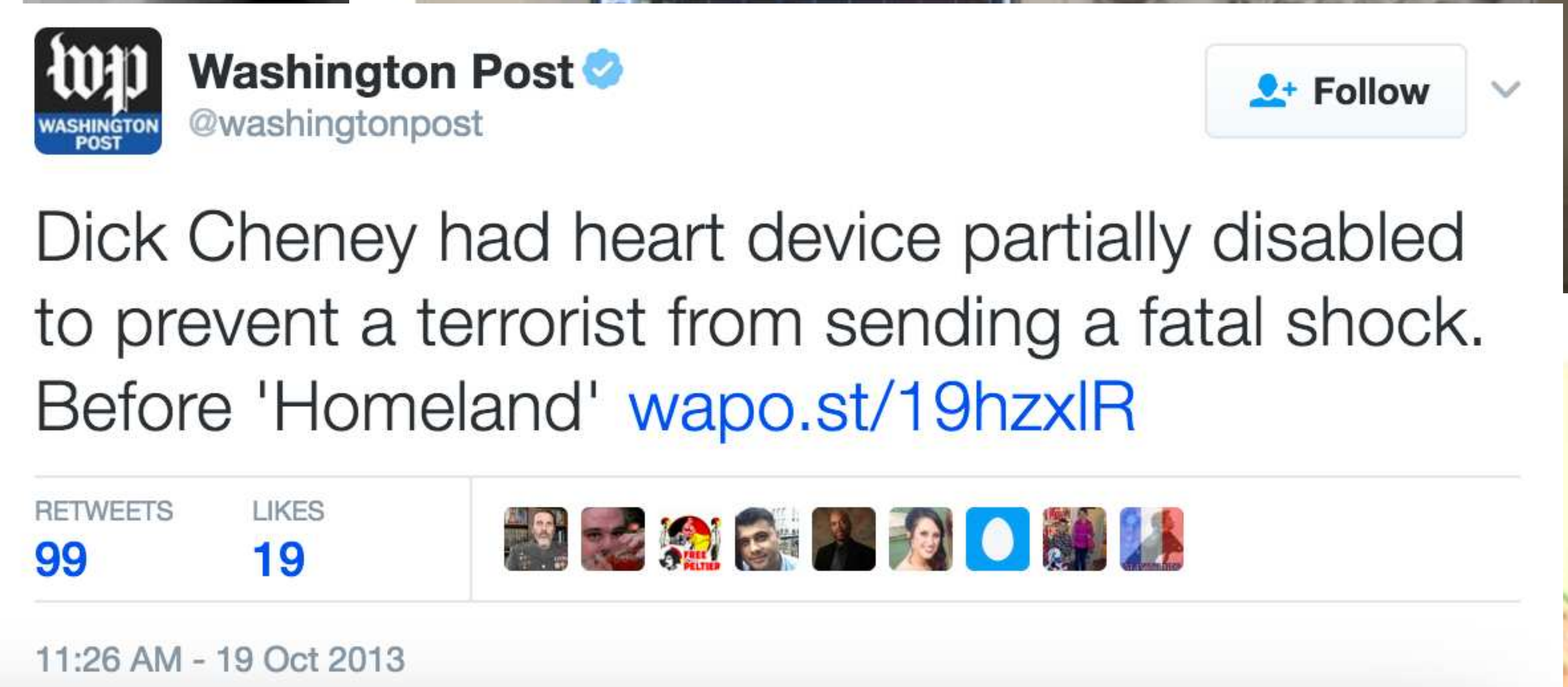






2
3
4
5
6
7
8
9

5
4
3
2
STANLEY

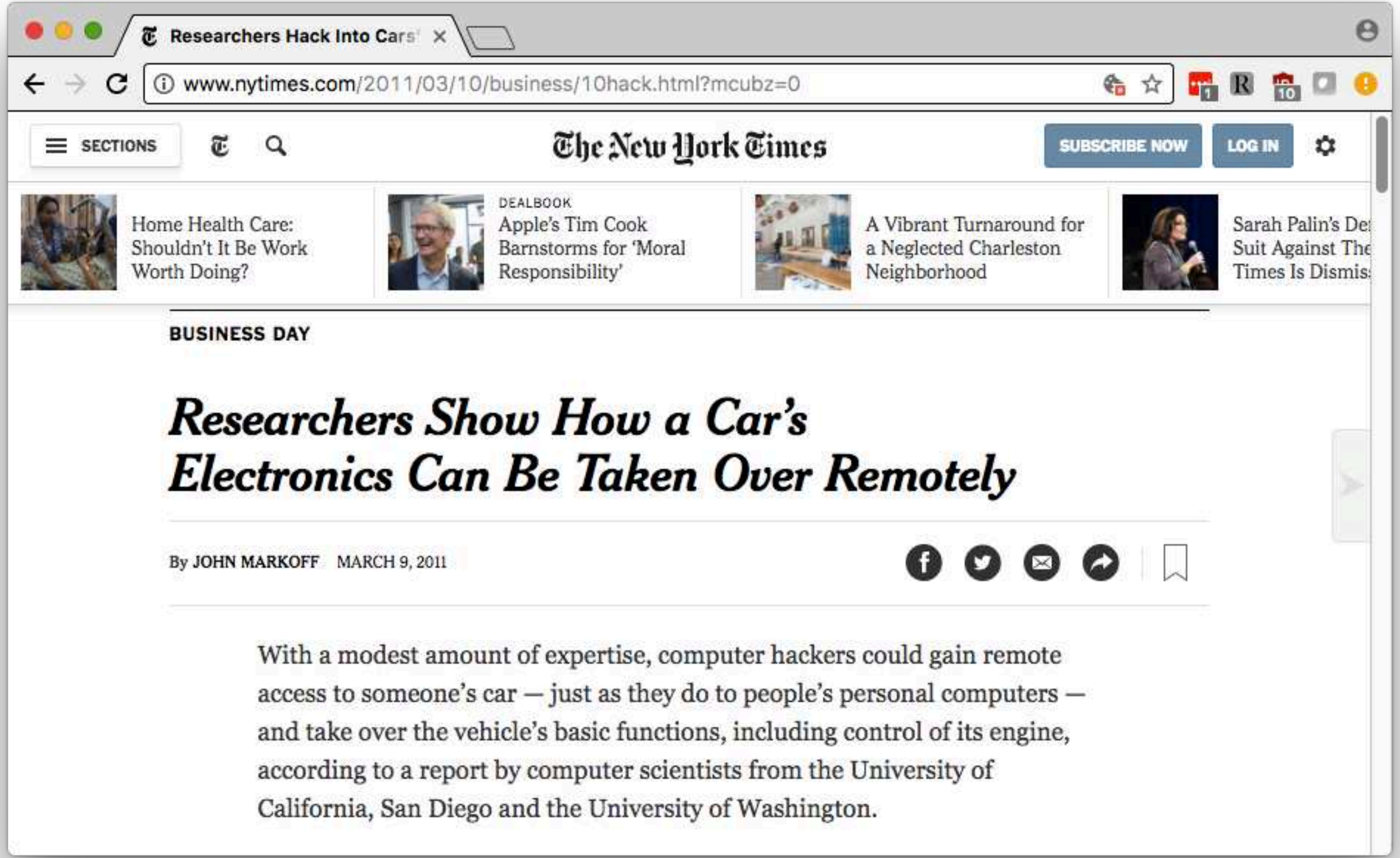


Washington Post
@washingtonpost

Dick Cheney had heart device partially disabled to prevent a terrorist from sending a fatal shock. Before 'Homeland' wapo.st/19hzxlR

RETWEETS 99 LIKES 19

11:26 AM - 19 Oct 2013


Researchers Hack Into Cars
www.nytimes.com/2011/03/10/business/10hack.html?mcubz=0
SECTIONS
The New York Times
SUBSCRIBE NOW
LOG IN

Home Health Care: Shouldn't It Be Work Worth Doing?

DEALBOOK
Apple's Tim Cook Barnstorms for 'Moral Responsibility'

A Vibrant Turnaround for a Neglected Charleston Neighborhood

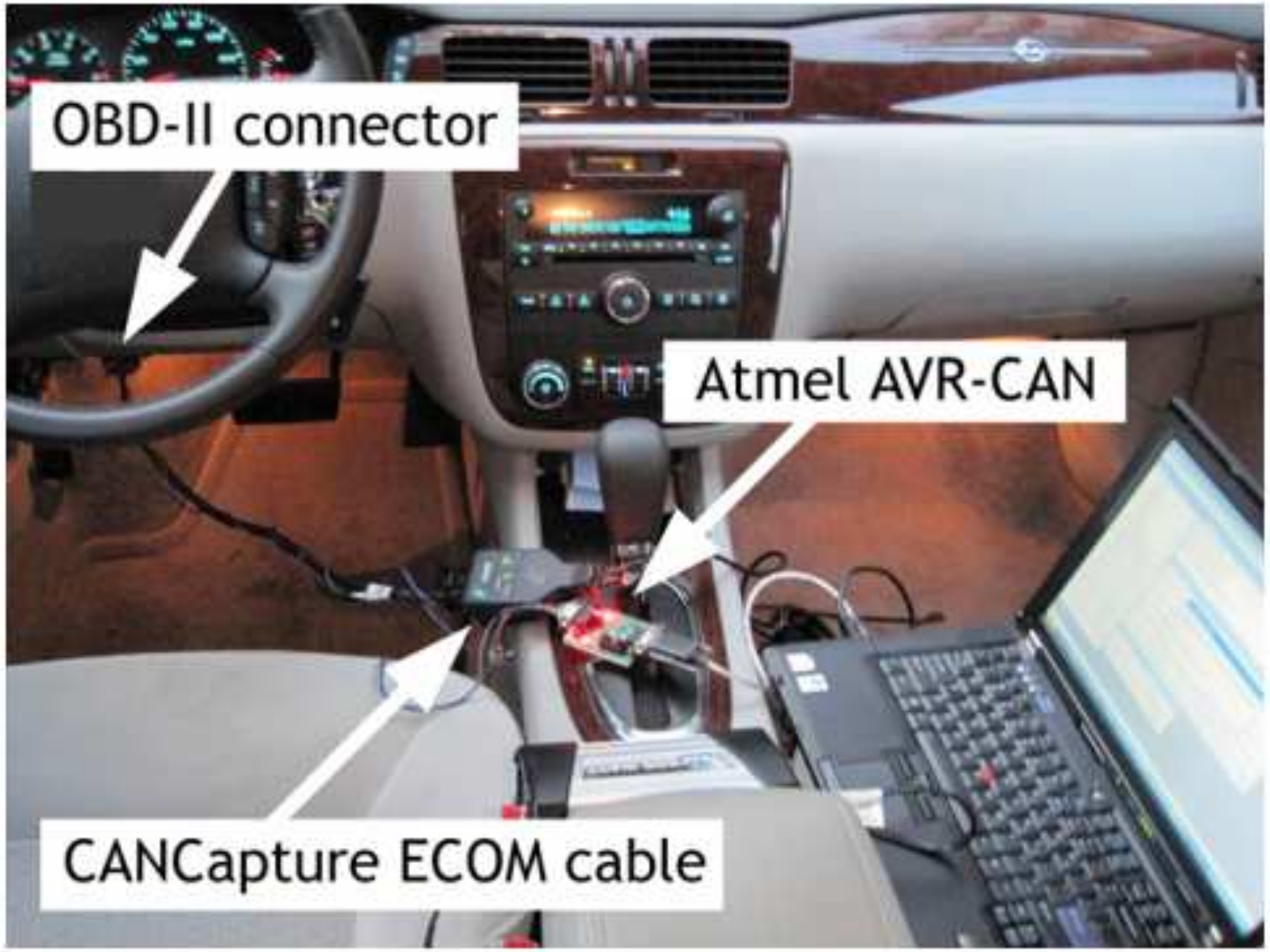
Sarah Palin's De
Suit Against The
Times Is Dismis

BUSINESS DAY

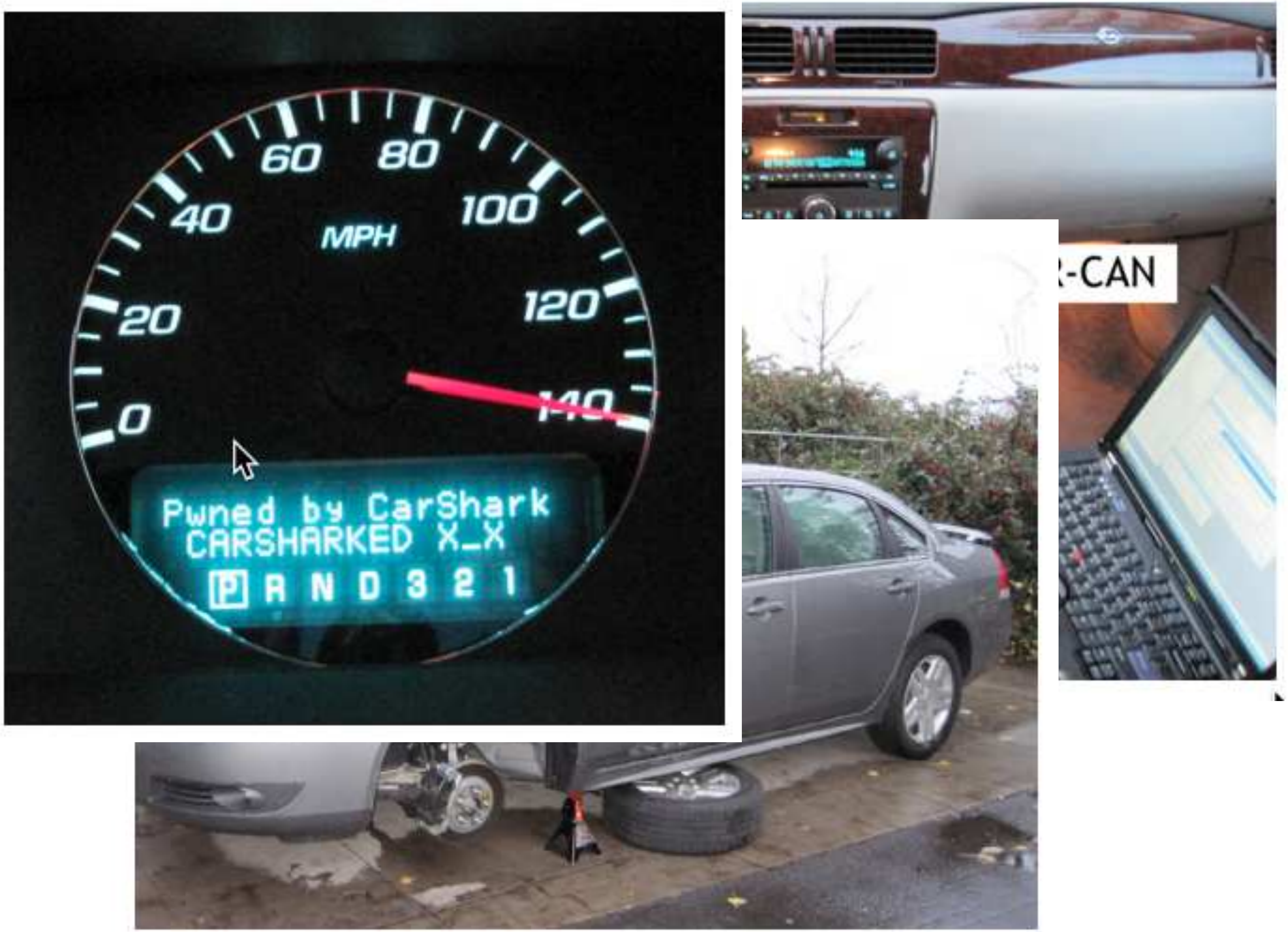
Researchers Show How a Car's Electronics Can Be Taken Over Remotely

By JOHN MARKOFF MARCH 9, 2011

With a modest amount of expertise, computer hackers could gain remote access to someone's car — just as they do to people's personal computers — and take over the vehicle's basic functions, including control of its engine, according to a report by computer scientists from the University of California, San Diego and the University of Washington.


OBD-II connector
Atmel AVR-CAN
CANCapture ECOM cable

OBD-II connector
-CAN



Pwned by CarShark
CARSHARKED X_X

Case Study: Reverse Engineering, Vulnerability Disclosure?

- Is this sort of reverse-engineering work ethical?
- Potential issues?

Wireless Eavesdropping

- A student in class creates a wireless network access point with no encryption or authentication and observes users who connect to it.
- Is this ethical?
- Potential issues?

Moving forward

- In this class you will not be asked to do anything that is illegal, unethical, or against university policy, so maybe you shouldn’t …
- Ask **permission** not forgiveness
- Principle of least surprise

To Learn More …

- http://www.icir.org/vern/cs261n/papers/burstein_legal_leet.pdf
- David Dittrich, Michael Bailey, Sven Dietrich. Building an Active Computer Security Ethics Community.
- Dittrich, David and Kenneally, Erin and Bailey, Michael, Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Menlo Report
- https://www.acm.org/about/code-of-ethics
- http://www.ieee.org/about/corporate/governance/p7-8.html
- https://www.eff.org/pages/grey-hat-guide
- http://www.cam.illinois.edu/viii/viii-1.1.htm

Questions?