

University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity


Cybersecurity Surveillance

CS 4950/5950
Homeland Security &
Cybersecurity


Lesson 40
Cybersecurity Surveillance

Rick White, Ph.D.
University of Colorado, Colorado
Springs



¹


1





University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Surveillance

- In the previous lesson we asked ourselves about going after cybercriminals and learned that it is a booming industry because **very few are caught**.
- It is not easy to trace the evidence from the crime scene to the criminal.
- In this lesson we are going to look at another aspect of this problem related to **cyber surveillance**.



²


2



Cyber Surveillance

- We start as before with the **1984 Counterfeit Access Device and Computer Fraud & Abuse Act** which makes it illegal to access a computer without permission from the owner.
- Of course we understand this to mean that **it is a crime to attempt to access somebody's personal computer or intercept Internet traffic coming and going from it.**



3

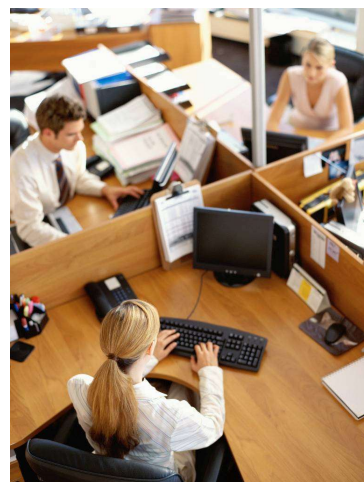
Esc

3



Cyber Surveillance


- **This law does not apply, however, to workplace computers.**
- The **1986 Electronic Communications Privacy Act** gives employers the **right to monitor the usage of their own property.**
- While local legislation varies, in general **it is legal for a company to monitor workplace computers, laptops and cell phones.**



4

Esc

4




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Cyber Surveillance

This law applies only to company property; **personal devices remain off limits.**



5 Esc

5




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Cyber Surveillance

- Companies may be motivated by the **desire to monitor employee performance, or to prevent them from engaging in activities that might get the company sued.**
- Either way, lawyers suggest developing a clear and reasonable monitoring policy, limiting monitoring to work related activities, and notifying employees that their work is subject to monitoring.



6 Esc

6




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Surveillance

What about government surveillance?



7 Esc

7



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Cyber Surveillance

- In 2013, Edward Snowden leaked information about the **PRISM** domestic surveillance program.
- PRISM was authorized by the **2007 Protect America Act** under the Bush Administration and was extended for five more years in 2012 under the Obama Administration.
- Congress put an end to the program in 2015**, however, after it was leaked by Snowden.



8 Esc

8




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Cyber Surveillance

PRISM was used to collect targeted internet communications in which at least one of the parties was outside the United States.



9
 Esc

9

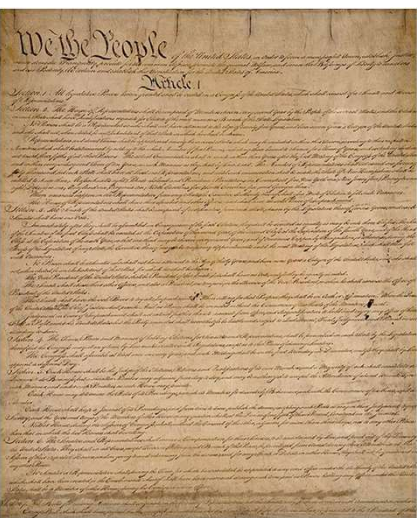


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Surveillance

As interpreted by the courts, the **Fourth Amendment** prevents surveillance of US citizens unless a warrant is issued citing probable cause.



10
 Esc

10

UCCS


University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity


Cyber Surveillance

- Such warrants may be obtained through special courts established by the 1978 **Foreign Intelligence Surveillance Act**.
- In 2008, FISA was amended to allow US intelligence agencies to conduct surveillance of US citizens for up to a week without obtaining a warrant.**
- PRISM used this authority to collect qualifying Internet communications.



11

Esc




**University of Colorado
Colorado Springs**

CS4950/5950

Homeland Security & Cybersecurity

Cyber Surveillance

- Collection was done by the FBI on behalf of the National Security Agency.**
- NSA would identify surveillance targets and send them to the FBI Data Intercept Technology Unit.
- The, FBI, in turn, would forward the list to Internet Service Providers together with a subpoena demanding they turn over the data.

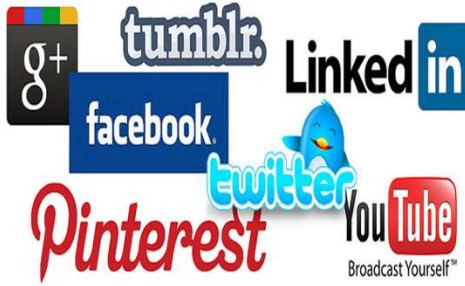


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Cyber Surveillance

- Corporate executives of several companies identified in the leaked documents said they had no knowledge of PRISM and **denied handing over such information to the government.**
- Such denials may be expected because **the FISA Amendment Act forbids companies from disclosing having received such an order** let alone acting upon it.



13
Esc

13




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Surveillance

Despite corporate denials and the fact Congress closed the program in 2015, allegations that Yahoo! had cooperated with NSA surveillance programs **threatened to overturn a \$4.8 billion sale to Verizon in 2016.**



14
Esc


14

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Surveillance

The point of this cautionary tale is that cybersecurity presents dangers from both sides; both from the good guys as well as the bad guys.



15
Esc


15

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



16
Esc

16