

## **TCOM 469: ELECTRONIC SURVEILLANCE AND CYBERCRIME**

Spring 2003, T, R 4-5.15 P.M.; OLSC 213

**Instructor: Dr. Peter Shields**

Office: 325 West Hall; tel: 372-8690; e-m: pshield@bgnet

Office hours: M, W 10A.M-12.30P.M.

### **COURSE OUTLINE AND OBJECTIVES:**

There is no doubt our lives are now subject to ever-greater means of surveillance that take a variety of forms. Electronically-based communications and information technologies have been heavily involved in this intensification of surveillance practices and processes. These technologies enable corporate and government organizations to collect and share massive amounts of information about our everyday lives -- our tastes, our preferences, our actions and our bodies. This has led many to conclude that we now live in a "Surveillance Society" where privacy is rapidly eroding and social divisions are being reinforced.

Paradoxically, at the same time as many electronically-based information and communication technologies have been involved in the intensification of surveillance practices, law enforcement and national security agencies have expressed concern that these technologies are actually undercutting their surveillance capabilities. They point out that major changes in the telecommunications sector, particularly the rapid digitization of telecommunications networks, the explosive expansion of the Internet, and the proliferation of strong private sector encryption are said to threaten law enforcement's ability to catch criminals. Without more surveillance and other regulatory responses, their argument runs, drug traffickers, terrorists, money launderers, pedophiles, as well as "digital" pirates will be able to operate with impunity and anonymity in "virtual" sanctuaries -- this will be devastating to public safety, national security, and the economy it is argued.

In this course, we will critically evaluate claims about the rise of the "Surveillance Society", the dangers of "cybercrime" and "cyberterrorism", and the demands for more electronic surveillance. We will also examine the responses to the growth in electronic surveillance. This will include an assessment of whether current US and international policy and legal frameworks are up to the challenges posed by the trends outlined above.

### **REQUIRED READING:**

- Reading packets on reserve in Jerome Library
- Book chosen to review

### **REQUIREMENTS AND EVALUATION:**

- Participation 10%
- Reaction Paper 10%
- Book Review 15%
- Research Paper 35%
- Research Paper Report 10%
- Take-home Final 20%

Participation: For the most part, this class will operate as a seminar, jointly facilitated by the instructor and the students. Informed participation is the key to a good participation grade. It is therefore imperative that you come to class prepared with questions and insights. Specifically, the participation grade is based on two elements: (i) the quality and consistency of your participation (ii) the written questions you submit at the beginning of each class period (two questions per reading).

It is my hope that our conversations/discussions in class do not end when class is over. Ideally, each of us should continue to think about issues that were discussed in class. Often this results in some additional insights and/or questions. To make sure we deal with ideas we generate after class, we will reserve the first few minutes of each class period for "old business." During that time, any of us may bring up topics covered in prior meetings, ask questions about previous discussions and readings, direct inquiries to the class and volunteer insights.

**Reaction Paper:** The reaction paper is a short paper (4-5 pages) in which you make an argument for your reactions to one or two ideas or an argument. This exercise is intended to help hone your skills at creating a good argument. Your ideas should be expressed in clear understandable statements. Remember, good arguments are based on a rationale. Ideally, you should be trying to integrate insights from the readings and class discussions into your papers.

- The reaction paper will be based on your reaction to the idea of the "panopticon" as applied to the electronic media.

**Due date: Feb. 4 at the beginning of class**

**Book Review:** The review, which should be 6 pages long, must include the following elements: description of the author's main arguments; assessment of what you perceive to be the author's most important points; critical evaluation of the author's arguments (did you think he/she did a good job? Why or why not?). Assume the author comes to class, what question(s) would you pose about his/her analysis?

You must choose a book from the following list (all are available via Ohiolink or from amazon.com):

- Brin, David. (1999). *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*. Reading, MA: Addison-Wesley.
- Andrews, Lori, & Dorothy Nelkins. (2001). *Body Bazaar: The Market for Human Tissue in the Biotechnology Age*. New York: Crown Publishers.
- Hubbard, Ruth and Elijah Wald. (1999). *Exploding the Gene Myth*. Boston: Beacon Press.
- Whittaker, R. (1999). *The End of Privacy*. New York: Norton.
- Rosen, Jeffrey. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.
- Gilliom, J. (2001). *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.
- Schulhofer, S.J. (2002). *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11*. New York: The Century Foundation Press.

**Due date: Mar. 4 at the beginning of class.**

**Research Paper:** This paper should be 10-12 pages. The research paper can be on a topic of your choice. The topic must be related in some way to the course. Here are four broad options from which you can choose (remember these are only examples):

*Option 1: Policy Evaluation:* What do you perceive to be the costs and benefits of the following policies -- remember to focus on the privacy implications. Should these policies be supported? If so, under what conditions?

1. Use of biometrics (e.g., electronic fingerscanning; retinal scans) to deter fraud.
2. Current patent laws permit scientists/doctors to patent genes without the informed consent of subjects. Is this an adequate approach?
3. The FBI's plans for a national genetic database.
4. The implementation of closed circuit television in public spaces.
5. Tracking web use over the internet, the use of "cookies" and other surveillance technologies on the internet.
6. Electronic billing for road usage and parking, electronic tracking of cars.
7. Proposal for a national identity card.
8. Electronic cash systems.
9. The Department of Defense's "Total Information Awareness Program."
10. The activities of credit reporting companies.
11. Electronically tagging for criminals and those on parole.

12. The USA Patriot Act – the national security versus civil liberty issues.
13. What should constitute digital piracy?

*Option 2: Policy Analysis of BGSU's Privacy Rules:* Critically assess BGSU's policy on student privacy (particularly as it relates to student's electronic records and communications). Develop what you consider to be a better set of privacy guidelines. Consider President Ribeau as your audience.

*Option 3: Policy Analysis of BGSU's New Infrastructure Project:* Examine the actual and potential surveillance capabilities of new telecommunications infrastructure. What are the privacy implications of the new infrastructure? Has the university adequately considered and planned for these implications? Consider President Ribeau as your audience.

*Option 4: Film Analysis:* Choose a film with a strong surveillance theme. Generally, the director will not highlight the privacy implications. Write an essay, beginning with your definition of privacy, that makes explicit the privacy implications of the story and identifies the surveillance paradigm of the director (e.g., are there elements of the panopticon?). Movies must be available on rental video. Relevant films include:

- *Fortress* (Director, Stuart Gordon)
- *Until the End of the World* (Director, Wim Wenders)
- *The Net* (Director, Irwin Winkler)
- *The Conversation* (Director, Francis Ford Coppola)
- *The Enemy of the State* (Director, Tony Scott)
- *Minority Report* (Director, Steven Spielberg)
- *Family Viewing* (Director, Atom Egoyen)

Whatever option you choose, the following applies:

- You must provide a one page proposal. The proposal should describe what you plan to do for the research paper assignment. More information on what I expect in this paper will be given in class.

**Proposal due date Mar. 18 at the beginning of class.**

**Research paper due Apr. 22 at the beginning of class.**

Research Paper Report: You are required to present your research paper. Each student will summarize their presentation on a 1-2 page hand-out. You will distribute the hand-out to the entire class and give a 10-15 minute report on the hand-out. Visual aids from film, TV, videos, magazines, and the web, for example, are strongly encouraged. Grading criteria include organization of presentation, clarity, professionalism and strength of conclusions.

**Presentation dates Apr. 22, 24, 29, May 1**

Take-home Final: Students will complete a take-home final. The final will be handed out on **April 24**. I expect that you can write this exam adequately in approximately 8-10 pages.

**Due date: May 8, Noon**

## GUIDELINES FOR PAPER AND GRADING POLICY

All papers should be typed and double-spaced. Use APA or Chicago style guidelines. Content, spelling and grammar are grading criteria. Bad grammar and/or bad spelling will result in the paper being returned without a grade. All papers (including the final) must have a complete reference list.

Extensions are given only for very unusual situations. All late work will be reduced in grade--half a grade point for each day late. The grading scale is as follows: A (90% and >), B (80%-89%), C (70%-79%), D (60%-69%), F (< 60%). "Incompletes" are not possible. Students are expected to be aware of the rules of academic misconduct set out in the University's Students Handbook, particularly those relating to plagiarism.

**WEEK-BY-WEEK OUTLINE**

Modifications may be made as the course progresses.

Jan. 14 (week 1)	Overview, objectives and expectations
Jan. 16, 21 (week 1/2)	<p>What is the panopticon? Is it useful for understanding the dynamics and social implications of electronic surveillance?</p> <ul style="list-style-type: none"> <li>• Lyon, D. (1991). "Bentham's Panopticon: From Moral Architecture to Electronic Surveillance," <i>Queen's Quarterly</i>, 98(3), pp. 596-608.</li> <li>• Lyon, D. (1994). "From Big Brother to the Electronic Panopticon," in D. Lyon, <i>The Electronic eye: The Rise of Surveillance Society</i>, Minneapolis: University of Minnesota Press, pp.57-79.</li> </ul>
Jan. 23, 28 (weeks 2/3)	<p>What is privacy? Do people really care about it?</p> <ul style="list-style-type: none"> <li>• Davies, S. (1997). "Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in P.E. Agre &amp; M. Rotenberg, eds, <i>Technology and Privacy: The New Landscape</i>, pp. 143-65.</li> <li>• Gotlieb, C. (1996). "Privacy: A Concept Whose Time Has Come and Gone," in D. Lyon &amp; E. Zureik, eds, <i>Computers, Surveillance and Privacy</i>, pp. 156-71.</li> </ul>
Jan. 30, Feb. 4 (weeks 3/4)	<p>Law enforcement and wiretapping:</p> <ul style="list-style-type: none"> <li>• Diffie, W., and S. Landau. (1998). "Communications: The Current Scene," in W. Diffie &amp; S. Landau, <i>Privacy on the Line: The Politics of Wiretapping and Encryption</i>. Cambridge, MA: MIT Press, pp. 183-203.</li> <li>• Schulhofer, S. J. (2002). "Enhancing Surveillance Powers, in S. J. Schulhofer, <i>The Enemy Within: Intelligence Gathering, Law Enforcement and Civil Liberties in the Wake of September 11</i>. New York: The Century Foundation Press, pp. 29-54.</li> </ul>
<b>Feb. 4 (week 4)</b>	<b>Reaction Paper Due</b>
Feb. 6 (week 4)	<p>Law enforcement and encryption:</p> <ul style="list-style-type: none"> <li>• Hager, N. (1996-97). "Exposing the Global Surveillance System," <i>CoverAction Quarterly</i>, 59, 11-17.</li> </ul>

- Denning, D.E and W. J. Baugh Jr. (2000). "Hiding Crimes in Cyberspace," in D. Thomas & B.D. Loader (eds) *Cybercrime: Law enforcement, Security and Surveillance in the Information Age*. New York: Routledge, pp. 105-131.

Feb. 11, 18 (weeks 5/6)

#### Digital Piracy

- Grabosky, P., Smith, R.G. and Dempsey, G. (2001). "Intellectual Property in Cyberspace" in Grabosky, P., Smith, R.G. and Dempsey, G. *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge: Cambridge University Press, pp. 130-142.
- Litman, J. (2001). "Choosing Metaphors" in Litman, J. *Digital Copyright*. New York: Prometheus Books, pp. 77-88.

**Feb. 13 (week 5)**

#### **No Class, Instructor Out of Town (Conference)**

Feb. 20, 25 (weeks 6/7)

#### Cyber-laundering

- Grabosky, P. and Smith, R.G. (1998). "Electronic Money Laundering" in Grabosky, P. and Smith, R.G. *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. New Brunswick, NJ: Transaction Books.
- Naylor, R.T. (2002). *Wages of Crime*. Ithaca, NY: Cornell University Press.

Feb. 27 (week 7)

#### Genetics and Surveillance

- Video: *Blue Genes*
- Hubbard, R., and W. Wald. (1999). "Of Genes and People" in *Exploding the Gene Myth*. Boston, Beacon Press, pp. 1-12.

Mar. 4 (week 8)

#### Genetics and Surveillance (cont'd)

- Andrews, L., and D. Nelkin. (1999). "DNA Identification and Surveillance Creep," *Sociology of Health and Illness*, 21 (5), pp. 689-706. This article can be read and/or downloaded from Ohiolink electronic journals via the following address:  
[www.bgsu.edu/colleges/library/infosrv/ejournal/ejhome.htm](http://www.bgsu.edu/colleges/library/infosrv/ejournal/ejhome.htm)

**Mar. 4 (week 8)**

#### **Book Review Due**

Mar. 6 (week 8)

#### Bio-commerce and Bio-prospecting

- Andrews, L., and D. Nelkin. (2001). *Body Bazaar: The Market for Human Tissue in the Biotechnology Age*. New York: Crown, pp. 24-63.

**Mar. 11 (week 9)**

#### **Spring break, No Class**

**Mar. 13 (week 9)**

#### **Spring break, No Class**

Mar. 18, 20 (week 10)

#### Workplace surveillance

- Regan, P.M. (1996). "Genetic Testing and Workplace Surveillance: Implications for Privacy," in D. Lyon & E. Zureik, eds, *Computers, Surveillance and Privacy*, pp. 21-46.
- Wood, Ann Marie. (1998). Omniscient Organizations and Bodily Observations: Electronic Surveillance in the Workplace. *International Journal of Sociology and Social Policy*, 18 (5-6), pp. 137-174). This article can be read and/or downloaded from BGSU electronic journals: [www.bgsu.edu/colleges/library/infosrv/ejournal/alpha.htm](http://www.bgsu.edu/colleges/library/infosrv/ejournal/alpha.htm)

**Mar. 18 (week 10)**

**Research Paper Proposal Due**

Mar. 25, 27 (week 11)

Surveillance of Public Spaces

- Rosen, J. (2001). "Being Watched: What Britain's Surveillance Experiment Can Teach Us About our Coming Security State." *The New York Times Magazine*, October 7.
- Surveillance of Public Spaces (cont'd)
- Woodward, J.D. (2001). *Super Bowl Surveillance: Facing Up to Biometrics*. Arroyo Center: Rand.

Apr. 1, 3 (week 12)

Militarization of law enforcement surveillance?

- Colonel Dunlap, C.J. (2001). "The Thick Green Line: The Growing Involvement of Military Forces in Domestic Law Enforcement." In P.B. Kraska (eds), *Militarizing the American Criminal Justice System*, Boston: Northeastern University Press, pp. 29-42.
- Haggerty, K.D. & R.V. Ericson (2001). "The Military Technostructures of Policing." In P.B. Kraska (eds), *Militarizing the American Criminal Justice System*, Boston: Northeastern University Press, pp. 43-64.

Apr. 8 (week 13)

Business Use of Transaction-Generated Information

- Gandy, O.H. Jr. (1995). It's Discrimination, Stupid! In J. Brooks & I.A. Boals (Eds.), *Resisting the Virtual Life: The Culture and Politics of Information*. San Francisco: City Lights, 35-47.

Apr. 10, 15, 17 (weeks 13/14)

Regulating surveillance practices

- Smith, J.H. (1994). "Solving the Problems," *Managing Privacy*, pp. 205-223.
- Bennett, C.J. (1997). "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" in P.E. Agre & M. Rotenberg, eds, *Technology and Privacy: The New Landscape*, Boston: MIT Press, pp. 99-123.
- Brin, D. (1998). Extracts from *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, MA : Addison-Wesley.
- Goldman, J. (1998). "Privacy and Individual Empowerment in the Interactive Age" in C.J. Bennett and R. Grant (eds) *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press, pp. 97-115.

<b>Apr. 22, 24, 29, May 1 (weeks 15/16)</b>	<b>Paper Presentations</b>
<b>Apr. 22 (week 15)</b>	<b>Research Paper Due</b>
<b>Apr. 24 (week 15)</b>	<b>Take Home Final Given Out</b>
<b>May 8 (week 17)</b>	<b>Final Exam Due, Noon</b>

The following are some helpful web sites:

Electronic Privacy Information Center, [www.epic.org](http://www.epic.org)  
Computer Professionals for Social Responsibility, [www.cpsr.org](http://www.cpsr.org)  
Electronic Frontier Foundation, [www.eff.org](http://www.eff.org)  
American Civil Liberties Union, [www.aclu.org](http://www.aclu.org)  
Federal Bureau of Investigation, [www.fbi.gov](http://www.fbi.gov)  
Federal Trade Commission, [www.ftc.gov](http://www.ftc.gov)  
Center for Democracy and Technology, [www.cdt.org](http://www.cdt.org)  
Privacy International, [www.privacyinternational.org](http://www.privacyinternational.org)  
Statewatch, [www.statewatch.org](http://www.statewatch.org)