

DISS 790 – Information Policy: Assignment C  
Information Haves vs. Have-Nots  
Information Policy in the Workplace  
Privacy: The Information Policy Brushfire of the Early 21<sup>st</sup> Century

by

Ronald G. Wolak  
wolakron@nova.edu

A paper submitted in fulfillment of the requirements  
for DISS 790 – Information Policy: Assignment C

School of Computer and Information Sciences  
Nova Southeastern University

November 2000

An Abstract of a Paper Submitted to Nova Southeastern University in Fulfillment of the Requirements for DISS 790 – Information Policy: Assignment C

DISS 790 – Information Policy: Assignment C  
Information Haves vs. Have-Nots  
Information Policy in the Workplace  
Privacy: The Information Policy Brushfire of the Early 21<sup>st</sup> Century

by  
Ronald G. Wolak

November 2000

The paper that follows was submitted to satisfy the requirements of DISS 790 – Information Policy: Assignment C. In the following pages, the paper completed the following assigned tasks:

1. Visit the anonymizer.com website. Read about their services. Surf the web, and view discussions about the services and report your results on these two activities
2. Read the first-in-the-nation anti-spam law, passed in Nevada in 1997 (located in an appendix in the Overly text). What are the possible drawbacks to a similar federal anti-spam law?
3. Draft a policy on employee e-mail use for your organization. If your organization already has a policy, how would you improve the existing policy? Be sure to include the essential elements regarding what privacy is afforded to employees, etc.
4. What are the pros and cons of having an explicit employee Internet policy?
5. Based on a recent study, the U.S. Federal Trade Commission is calling for the enactment of a series of federal laws related to Internet privacy. Do you agree or disagree with the FTC's recommendations? What are the possible ramifications of such new laws? Should the private sector be given more time to establish effective self-regulation practices?
6. Draft a privacy statement for your organization's web site. If your organization already has such a statement, how would you modify the policy to improve it based on the principles of privacy that you have learned in class and in your readings? Be specific and provide sample language.
7. Briefly, describe the points on which the U.S. and the EU agreed to resolve the long-standing data privacy rules dispute. Should the U.S. government adopt, in totality, the principles behind the European Commission Privacy Directive? Why or why not?
8. What are the advantages of "universal service"; what are its drawbacks or implications?
9. Is the Digital Divide a legitimate concern in the U.S. or merely an outgrowth of partisan politics? What role should the U.S. government play in bridging the so-called "digital divide"? How serious is the "digital divide", internationally? Give examples.

## Table of Contents

<b>Abstract</b>	ii
<b>1. Task 1</b>	1
<b>2. Task 2</b>	4
<b>3. Task 3</b>	7
<b>4. Task 4</b>	12
<b>5. Task 5</b>	17
<b>6. Task 6</b>	20
<b>7. Task 7</b>	25
<b>8. Task 8</b>	28
<b>9. Task 9</b>	32

## Task 1

**Visit the anonymizer.com website. Read about their services. Surf the web, and view discussions about the services and report your results on these two activities**

Anonymizer.com is one of a number of anonymous proxy services that allow users to surf the Internet anonymously. The company's mission is to ensure that online activity does not compromise an individual's right to privacy (Anonymizer, 2000). In general, anonymous proxy services are classified into three types: Web-based, direct, and client (WebVeil, 2000). Web-based proxies, such as anonymizer.com, use server-side programs to enable users to surf anonymously using a standard Web-browser. There is nothing to download, install, or configure. In contrast, direct and client proxy services require either custom browser configuration or the installation of client-side applications to mask a user's surf activity.

The anonymizer.com site offers free basic service that protects a user's identity by hiding his/her IP address. The service also prevents visited Web sites from using cookies, Java, JavaScript, and other forms of information gathering to track a user's Web activity. Premium paid services offered by the site include Safe Cookies, URL encryption, anonymous downloads, secure connections, anonymous e-mail, newsgroup access, Web publishing, secure tunneling, and dialup access.

Anonymizer.com makes cookies "safe" by encrypting and repackaging them to prevent their use in tracking a user's browsing habits. Other premium services, URL encryption and anonymous downloads, prevent ISPs from logging the sites a user visits by encrypting all browser and file download requests. Anonymizer.com also provides secure shell (SSH) access to their servers. This secure tunneling technology provides users with secure e-mail, newsgroup access, and Web publishing. Anonymizer.com

encrypts all Internet activity between a user's computer and its servers. This prevents firewall monitoring programs, ISPs, and Internet routing devices from monitoring a user's activities.

Anonymizer.com also offers a product called Window Washer, which is available for download from the Web site (Harrison, 2000). The program removes all traces of Internet activity from a user's computer. Window Washer runs silently in the background removing activity information from the user's browser, office applications, and operating system. In addition, a bleaching feature allows users to destroy files. This renders them unrecoverable by unerase and undelete software utilities.

The basic service offered by Anonymizer.com allows users to sample the service from an URL address box located on their Web site. The service is limited and meant to entice users to sign up for a premium account. Drawbacks include a built-in ten second delay before accessing an Internet address, and a one third page banner advertisement that occupies the top of every Web page. In addition, URL encryption and safe cookies are disabled.

Internet discussion groups speak highly of Anonymizer.com (eGroups, 2000). In fact, one group discussed the effectiveness of the product during the conflict in Kosovo. Kosovars and Serbs used the service, along with a Kosovo e-mail system, to report conditions and human rights violations from within the war zone. In addition, discussion groups in China and the Middle East use Anonymizer.com to post information censored by their governments (Melugin, 2000).

In conclusion, a 30-day free trial of Anonymizer.com's premium services would have been a more effective way of sampling the company's privacy applications. The free

basic service offered on the company's Web site did not convince the author to subscribe and spend money.

## References

- Anonymizer (2000). Anonymizer.com: Privacy is Your Right. *Anonymizer.com*.  
<http://www.anonymizer.com/corporate/index.shtml>. Accessed November 8, 2000.
- eGroups. (2000). Anonymizer.com.  
<http://www.egroups.com/search?query=anonymizer.com>. Updated November 12, 2000. Accessed November 12, 2000.
- Harrison, A. (2000, August 7). Carnivore: How much bite behind the bark?  
*Computerworld*, 34, 73.
- Melugin, J. (2000, September). Consumers can find privacy on-line. *Consumers' Research Magazine*, 83, 20-21.
- WebVeil (2000). Anonymous Proxy Services. *WebVeil.com*.  
<http://webveil.com/matrix.html>. Updated November 7, 2000. Accessed November 12, 2000.

## Task 2

**Read the first-in-the-nation anti-spam law, passed in Nevada in 1997 (located in an appendix in the Overly text). What are the possible drawbacks to a similar federal anti-spam law?**

The quantity of spam e-mail received by users during the past year has grown at an astounding rate (Halcon, 2000). Experts from Brightmail, Inc. reported that the company is intercepting an average of 4,900 junk e-mail attacks per day. This is 400 percent higher than last year. In addition, a survey conducted last year by the Gartner Group reported that 90 percent of e-mail users receive spam at least once a week and 50 percent receive it more than six times a week (Abrams, 2000). There are five basic solutions to the spam problem: social pressure, economic disincentives, technical means, legal action under existing laws, and new legislation.

New legislation is probable the most risky and uncertain of the five solutions because of unknown side effects. For example, in 1997 the Senate passed an anti-spam rider on an unrelated bill covering telephone “slamming” (Catlett, 1998). Internet experts widely agreed the rider would be worse than the status quo because it would legitimize spam. In addition, free-speech advocates warn against government restrictions on electronic messaging. They contend that under existing laws spam recipients can sue unscrupulous e-mailers. The challenge they say is to balance the privacy of users with the free speech rights of marketers.

Despite the risks, state governments are passing anti-spam laws. Nevada chose to limit spam with new legislation and became the first state to enact an anti-spam law in 1997. Washington and California subsequently passed similar anti-spam laws. However, a county court judge in Washington declared the new Washington law to be

unconstitutional under the Interstate Commerce Clause (Marcotte, 2000). The judge found that for businesses not to violate the law they would have to determine if any of the e-mail recipients did not live in the state of Washington. In the judge's opinion, this would be unduly restrictive and burdensome and would hurt consumers and legitimate businesses. In support, critics of state-level anti-spam legislation contend that federal government regulation would be best since the Internet is such a broad area. However, by that argument, would not international anti-spam regulation be even better?

At the federal level, the "Unsolicited Commercial Electronic Mail Choice Act of 1997" did not attempt to ban spam but rather to force such mail to be identified in an easily filtered manner (Cranor & LaMacchia, 1998). Recently, the House of Representatives passed e-mail legislation by an almost unanimous vote (Bray, 2000). The bill requires anyone sending unsolicited commercial e-mail to include a valid return address. This would allow recipients to reply and have their names removed from future mailings. In addition, the Federal Trade Commission is able to bring legal action against spam senders violating the provisions of the legislation. Internet Service Providers (ISPs) are also able to sue spammers in federal court. Penalties, if convicted, would range from \$500 to \$50,000 per illegal message.

Have the state laws been effective? In 1999, Brightmail analyzed ten million pieces of spam and found virtually no compliance with existing state laws (Brown, 2000). This raises questions whether a federal law modeled after the state laws would perform any better. Many now believe that the future of spam suppression lies with technology that allows ISPs to identify and remove spam quickly before it reaches a user's inbox.

In conclusion, the drawbacks of both federal and state anti-spam legislation

include side effects such as legitimizing spam and limiting the rights of marketers. In addition, anti-spam legislation could limit legitimate anonymous communications. The characteristics of e-mail that make it so appealing to mass marketers also make it an effective tool for academic communities, political organizers, social networks, and individuals. Should anti-spam legislation be state, federal, or international? The question becomes mute when users and ISPs employ advanced filtering technology to dispose of unwanted e-mail.

### References

- Abrams, J. (2000, July 19). Bill would shackle junk e-mail. *Florida Today*, pp. 4.
- Bray, H. (2000, August 24). Choosing spam over censorship. *Boston Globe*, pp. C1.
- Brown, D. (2000). Anti-Spam Forces Gaining Ground. *Inter@ctive Week*.  
<http://www.zdnet.com/filters/printerfriendly/0,6061,2569928-2,00.html>. Updated May 16, 2000. Accessed November 17, 2000.
- Catlett, J. (1998, November 1). What can be done about junk e-mail? *USA Today Magazine*, 127n.
- Cranor, F., & LaMacchia, B. (1998). Spam! *Communications of the ACM*, 41(8).
- Halcon, C. (2000). Spam Attacks At All-Time High. *Brightmail*. <http://www.brightmail.com/company/media/press/pr26.shtml>. Updated October 27, 2000. Accessed November 17, 2000.
- Marcotte, J. (2000). Judge Cans Washington's Spam Law. *Government Technology News*.  
<http://www.govtech.net/news.phtml?docid=2000.03.17-1025000000000022>. Updated May 17, 2000. Accessed November 8, 2000.

### Task 3

**Draft a policy on employee e-mail use for your organization. If your organization already has a policy, how would you improve the existing policy? Be sure to include the essential elements regarding what privacy is afforded to employees, etc.**

American Axle and Manufacturing (AAM) is a tier one supplier of automotive driveline systems (AAM, 2000). Headquartered in Detroit, Michigan, AAM has five North American manufacturing facilities. The company's near-term plans include expansion in Europe, Asia, and South America. AAM employs more than 8,500 associates.

AAM's information technology infrastructure includes a state-of-the-art electronic messaging system that facilitates both internal and external communication. Employee misuse of the company's e-mail system could have serious consequences (i.e. employee harassment and claims of a hostile environment, disclosure of trade secrets, copyright and criminal penalties, and a lessening of the company's position in litigation) (Gall, 2000). In light of the above, the author presents the following draft of an e-mail use policy for AAM. Key points covered in the policy are:

- The e-mail system belongs to AAM
- Employees have no expectation of privacy
- The e-mail system is to be used for work-related items only
- AAM may conduct occasional monitoring of system activity
- Passing offensive materials will result in discipline or termination
- Employees may not transmit AAM information without the permission of a designated AAM official.

Since promulgation and employee awareness of the e-mail policy are two of the most

important considerations, all e-mail users will be required to sign the acknowledgment given below (Grillo & Linderman, 1998). In addition, before logging into the system, a short message box will remind users of the policy and require them to once again agree to its conditions. The following is a sample e-mail policy for use by AAM:

## American Axle & Manufacturing Corporate E-mail Use Policy (DRAFT)

### **Statement of Purpose**

This policy describes American Axle & Manufacturing's (AAM's) guidelines with regard to access to and disclosure of electronic mail (e-mail) messages sent to or received by AAM employees using of the AAM e-mail system. The policy applies to all AAM employees. AAM will execute the policies given below, but reserves the right to modify them at any time in response to changing conditions. This policy is applicable to both internal and external (Internet) e-mail.

AAM maintains the e-mail system to facilitate the transaction of company business. The e-mail system hardware is company property, and all messages composed, sent, or received on the system are, and remain, the property of the company. Questions about this policy should be brought to the attention of your supervisor or your local human resources department.

### **Permissible Use**

1. The use of the e-mail system is reserved solely for the conduct of company business. It may not be used to conduct personal business.
2. No e-mail may be sent which attempts to hide the identity of the sender, or represent the sender as someone else or from another company.
3. E-mail should not be used in a manner likely to cause network congestion or restrict the ability of other users to access and use the system.
4. E-mail messages sent by an employee to one or more individuals outside the company are statements identifiable and attributable to the company. Although some users include personal disclaimers in messages, there is still a connection to the company. All e-mail sent by employees must comply with this and other company policies and may not disclose confidential or proprietary company information.
5. The use of Web-based e-mail services (e.g. Hotmail.com) is strictly forbidden due to the risk of viruses in unscreened downloads and the inability of the company to monitor such correspondence.

6. The e-mail system may not be used in a way that is insulting, disruptive, offensive, or harmful to the morale of other persons. Examples of this type of prohibited e-mail content include sexually explicit jokes or cartoons, ethnic or racial slurs, or any other message that can be construed to be harassment or disparagement of others based on their sex, race, religion, sexual orientation, age, national origin, or political beliefs.
7. E-mail system users are prohibited from the unauthorized use of the password or encryption key of another employee to access that employee's e-mail messages.
8. The e-mail system shall not be used to upload or download copyrighted materials, proprietary financial information, trade secrets, or similar material without approval.
9. The e-mail system may not be used to solicit for religious or political causes, commercial ventures, outside organizations, or other personal correspondence.

### **Monitoring and Enforcement**

1. The company has and will exercise the right to audit, intercept, access, review, and disclose all information on the company's e-mail systems at any time. Such access may occur during or after working hours, with or without employee notice. The contents of e-mail, properly obtained for legitimate business purposes, may be disclosed within the company without the permission of the employee.
2. Messages on the e-mail system are not confidential. The use of passwords for security does not guarantee confidentiality. Even deleted messages may be retrieved and read. All passwords or pass codes must be disclosed to the company. No password or pass code may be used that is unknown to the company.
3. Any employee who is aware of violations of this policy shall notify the e-mail system administrator at emailadmin@aam.com.
4. Any employee found to abuse the privilege of using AAM's e-mail system and violating this policy shall be subject to discipline, up to and including discharge.

### **Acknowledgement**

As an employee of American Axle & Manufacturing, Inc., I, \_\_\_\_\_, recognize and understand that the company's e-mail systems shall be used only for

conducting company business. I understand that the use of this equipment for private purposes is strictly prohibited and agree not to use a password that has not been disclosed to company. Further, I agree not to access a file or retrieve any stored communication other than where authorized or an authorized company representative has given prior permission.

I also understand that the company has and will exercise the right to audit, intercept, access, review, and disclose all information on the company's e-mail systems at any time. Such access may occur during or after working hours, with or without employee notice. In addition, I am aware that passwords do not restrict the company's right to access all information contained in company e-mail systems. I am also aware that violations of this policy may subject me to disciplinary action, up to and including discharge from company employment.

I have read and understand the company's e-mail use policy located in Information Technology Policies Manual. I have read and understand this notice.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

### **Improvements to the Existing AAM E-mail Use Policy**

The AAM Electronic Mail Policy INF-12-007 (1998) is an excellent example of a company e-mail policy. The five-page policy document covers all topics included in the "Permissible Use" and the "Monitoring and Enforcement" sections above. However, the policy lacks of a signed acknowledgement statement. This oversight will be brought to the attention of the AAM CIO.

### **Conclusion**

In conclusion, a well-written e-mail policy is the first step in ensuring the proper and effective use of a company's electronic messaging infrastructure. Promulgation and employee awareness of the policy are also important.

### **References**

AAM. (2000). Driving Performance. *AAM.com*. <http://www.aam.com/about/index.html>. Updated September 29, 2000. Accessed November 19, 2000.

Curry, F. (1998). *AAM - Electronic Mail Policy (INF-12-007)*. Detroit: American Axle & Manufacturing.

- Gall, B. (2000). Company E-mail and Internet Policies. *Gigalaw.com*.  
<http://www.gigalaw.com/articles/gall-2000-01-p1.html>. Updated January, 2000.  
Accessed November 19, 2000.
- Grillo, J., & Linderman, J. (1998). Crafting a Policy on Employee E-mail.  
<http://www.beyondcomputingmag.com/1998/03-98/ethics.html>. Updated April,  
1998. Accessed November 5, 2000.

## Task 4

### **What are the pros and cons of having an explicit employee Internet policy?**

A report by the Aberdeen Group found that corporations without employee Internet policies expose themselves to significant legal liabilities, bandwidth abuse, and employee productivity gaps (Butler, 2000). In addition, reports from the FBI and independent researchers support this conclusion and identify employees as the single highest risk and the most common cause of data loss, network abuse, and litigation.

According to the Gartner Group, 75 percent of companies with more than 1,000 employees will have Internet usage policies by 2001 (Yasin, 1999). While explicit Internet policies provide a number of benefits to companies and their employees, they also have a number of disadvantages. The following sections explore some of the pros and cons of employee Internet policies.

#### **Pros**

Explicit Internet policies provide a company with three major benefits. Those benefits include increased employee productivity, decreased demand on network bandwidth and resources, reduced legal liability, and increased protection of trade secrets

#### *Increased Employee Productivity*

Recent studies have found that the average employee at work uses the Internet for personal use at least three hours per week (Overly, 1999). In addition to this direct loss of productivity, increased network and application response times indirectly affect other employees. Employee Internet policies reduce the personal use of the Internet and result in increased employee productivity. Companies that have implemented employee Internet policies have also found that employees respond better when they know where they stand

and what the company expects from them (Gaudin, 1999).

#### *Decreased Demand on Network Bandwidth and Resources*

Non-business usage of the Internet by employees significantly increases a company's IT costs (Butler, 2000). In addition to the cost of wasted time caused by slow network response or unreliable connections, excessive misuse results in increased spending to provide unnecessary leased lines, routers, and disk storage. For example, one company lost 40 percent of its bandwidth when a handful of employees downloaded an Internet screen saver that required constant updates from the Internet (Overly, 1999). Companies that implement explicit Internet policies along with acceptable use monitoring software are able to decrease significantly the demand on network bandwidth and resources.

#### *Reduced Legal Liability*

The implementation of an explicit employee Internet policy also reduces a company's legal liability from illegal employee behavior (e.g. harassment and sexual discrimination) (Gaudin, 1999). Although a good percentage of companies do not have policies, court rulings indicate that if a company wants to avoid punitive damages, it must create Internet policies that keep employees within the law. In addition, companies must ensure that employees understand those policies.

For example, two recent court cases (i.e. Kolstad versus The American Dental Association and EEOC versus Wal-Mart Stores) set precedents in this area. In both cases, the companies were found liable for their employees' inappropriate behavior on the job.

#### *Increased Protection of Trade Secrets*

A properly drafted employee Internet policy should remind employees that it is

their duty to protect company trade secrets (Overly, 1999). The theft of trade secrets is a growing problem in the United States. In 1992, U.S. companies estimated their losses from the theft of trade secrets to be \$1.8 billion. For example, unpublished teaching materials of the Church of Scientology lost their status as trade secrets when they became available on the Internet.

### **Cons**

In addition to their benefits, Internet usage policies present companies and employees with a few disadvantages. These include increased company responsibility, decreased employee morale, loss of employee privacy, and loss of productivity.

#### *Increased Company Responsibility*

Companies with Internet policies that outline the companies' ability to access and monitor employee Internet activity may have an increased duty to protect employees from material that creates a hostile environment (Overly, 1999). In fact, companies with greater control over employee Internet activity are more likely to be held liable if they fail to detect and remove offensive content. When companies with such policies detect inappropriate content, they should act quickly to remove it.

#### *Decreased Employee Morale*

When a company plays Big Brother and implements and enforces an extreme employee Internet policy, the impact on employee morale may be negative (Yasin, 1999). In fact, Lance Cottrell, CEO of Anonymizer.com, commented that a number of businesses are overreacting to the personal use of the Internet by their employees (Murphy, 2000). He reasons that workers need to take breaks, and they will take them either at the water cooler or at their desks.

### *Loss of Employee Privacy*

Another key reason that companies institute Internet policies is to make it clear to employees that the equipment, networks, systems, and data they use and create are company property, and that employees have no privacy (Overly, 1999). In order for an employee to win a claim for invasion of privacy, the employee must establish the expectation of privacy in the workplace. Employee Internet policies decrease the validity of such claims.

### *Loss of Productivity*

An overzealous Internet policy can be just as harmful as a nonexistent one (Yasin, 1999). For example, one TV station's stringent blocking of Internet sites hampered the company's art department from doing its job. The department was unable to download graphic art from a drug-enforcement agency site because the Internet site filtering software the TV station was using identified the agency as a "drug" site.

### **Conclusion**

In conclusion, although explicit Internet policies provide a number of benefits to companies and employees, they also have a number of disadvantages. A few of the benefits are increased employee productivity, decreased demand on network bandwidth and resources, reduced legal liability, and increased protection of trade secrets. Disadvantages include increased company responsibility, decreased employee morale, loss of employee privacy, and loss of productivity.

### **References**

Butler. (2000). Internet Usage Monitoring and Reporting. *Butler.org*.  
<http://www.butler.org/bhis/policy/internet.html>. Updated August 9, 2000.  
Accessed November 19, 2000.

- Gaudin, S. (1999). The Perils of Privacy. *Network World*.  
<http://www.nwfusion.com/power99/power99-privacy.html>. Updated December 27, 1999. Accessed November 5, 2000.
- Murphy, C. (2000). More Companies Keep Eye on Employee's Messages. *InformationWeek*.  
<http://www.informationweek.com/shared/printArticle?article=infoweek/786/monitor.htm&pub=iwk>. Updated May 15, 2000. Accessed November 19, 2000.
- Overly, M. (1999). *E-policy: How to develop computer, e-mail, and Internet guidelines to protect your company and its assets*. New York: American Management Association.
- Yasin, R. (1999). Web Slackers Put On Notice. *InternetWeek*.  
<http://www.internetwk.com/lead/lead101599.htm>. Updated October 15, 1999. Accessed November 21, 2000.

## Task 5

**Based on a recent study, the U.S. Federal Trade Commission is calling for the enactment of a series of federal laws related to Internet privacy. Do you agree or disagree with the FTC's recommendations? What are the possible ramifications of such new laws? Should the private sector be given more time to establish effective self-regulation practices?**

The term “privacy” is sometimes defined as the right to be left alone (Wang, Lee, & Wang, 1998). In the context of the electronic marketplace, privacy often refers to personal information. The usual interpretation of the invasion of privacy is the unauthorized collection, disclosure, or use of personal information obtained during e-commerce transactions. Earlier this year, the Federal Trade Commission (FTC) issued a report calling on Congress to pass broad legislation covering online privacy (Perine, 2000). In the report, the majority of the five-member commission found that industry self-regulation of online privacy was lacking.

Appearing before a Senate committee, FTC Chairman Robert Pitofsky applauded the progress of industry self-regulation but said it fell short of the effectiveness of programs that have the rule of law to back them up. The report called for federal regulation of the way Internet companies collect and use information about their customers. This marked an important shift in FTC policy, which had previously agreed with Internet Industry arguments that self-regulation was the most effective way to protect public privacy rights.

The FTC’s recommendations are a positive step toward the protection of Internet privacy. Industry self-regulation has continually demonstrated itself to be inadequate (Clarke, 1999). During 1995-98, the FTC examined the behavior of corporate Web sites and found that effective self-regulatory systems did not emerge. This is in spite of the fact

that consumers identify the loss of personal privacy as the most crucial e-commerce issue. The information economy is dependent on trust, and industry self-regulation efforts have fallen short in this area. The industry has had ample time to address the problem, and now federal law should bolster self-regulation efforts.

Government, businesses, and individuals each play a role in protecting Internet privacy (Wang et al., 1998). Privacy protection must be a joint effort of the three groups. The government's role is to promote strong privacy laws for the private and public sectors. Independent privacy commissions should oversee the implementation of these laws, encourage industry self-regulation, and educate the public on privacy issues. The role of business is to promote self-regulation that fosters fair information practices. Finally, individuals are able to protect their privacy by implementing privacy enhancing technologies such as those developed by Anonymizer.com and Zeroknowledge.com (Melugin, 2000).

In the absence of a unifying framework of federal privacy statutes, public confidence in matters of online privacy will continue to decrease (Clarke, 1999). One ramification would be a slowdown in the growth of e-commerce. Businesses and governments in most advanced countries attribute the slow adoption of e-commerce to a severe lack of consumer trust. Lack of consumer confidence is bad for business.

Furthermore, self-regulation is unable to enforce privacy regulations without a widely recognized accreditation system (Wang et al., 1998). This hinders a consumer's ability to choose a creditable Internet merchant and results in a chaotic environment similar to the Internet market of today. It is also important that privacy enhancing technology, industry self-regulation, and legislation be coordinated to provide a privacy

framework that serves individual privacy concerns and business e-commerce initiatives. While self-regulation is not enough, it is also important to ensure that any legislation enacted does not limit consumer choice or provide a disincentive for the development of future technology (Melugin, 2000).

In conclusion, the Internet presents a severe threat to personal privacy. The U.S. must join the rest of the world in recognizing the role that legislation plays in establishing a privacy-protective framework for the Internet economy.

### **References**

- Clarke, R. (1999). Consumer privacy concerns about Internet Marketing. *Communications of the ACM*, 41(3), 63-70.
- Melugin, J. (2000, September). Consumers can find privacy on-line. *Consumers' Research Magazine*, 83, 20-21.
- Perine, K. (2000). FTC Backs Its Online Privacy Report. *The Industry Standard*. <http://www.thestandard.com/article/display/0,1151,15439,00.html>. Updated May 25, 2000. Accessed November 5, 2000.
- Wang, H., Lee, M., & Wang, C. (1998). Consumer privacy concerns about Internet Marketing. *Communications of the ACM*, 41(3), 63-70.

## Task 6

**Draft a privacy statement for your organization's web site. If your organization already has such a statement, how would you modify the policy to improve it based on the principles of privacy that you have learned in class and in your readings? Be specific and provide sample language.**

In June 1998, the Federal Trade Commission (FTC) reported the details of a survey of 1400 Web sites (Kane & McEahern, 2000). The survey found that the vast majority of the sites, almost 85 percent, collected personal information from consumers. Only 14 percent of the random sample of sites provided a notice of their information practices. In addition, less than two percent provided a comprehensive privacy policy. A more recent study conducted by PC Data Online in February 2000 found that 630 sites among the Top 1000 posted a comprehensive privacy policy. This is an improvement of 30 times in less than two years.

Web site privacy policies explain the responsibilities of the organization that is collecting personal information and the rights of the person who provided the information (EPIC, 1997). Typically, the organization will explain why the information is collected, how it is used, and what steps will be taken to keep the information private. In addition, individuals are able to obtain their data and make any necessary corrections. Strong privacy practices give Web site visitors the assurance that personal information will not be misused. It also encourages the growth of e-commerce. The following are five important characteristics of a well-written Web site privacy statement (Rotenberg, 1999):

1. The privacy policy should be available and easy to find – preferably on the home page linked to the word “privacy.”
2. Privacy policies should spell out how and when personal information is collected.
3. Site visitors should have access to view and edit their personal data.

4. Sites should notify visitors that cookies containing information about the user placed on the user's system.
5. Web sites should support anonymous access.

In addition to the above, global companies like American Axle & Manufacturing (AAM) must be sensitive to foreign privacy policies such as the European Union's (EU's) Privacy Directive. Compliance with the recent "safe harbor" agreement between the U.S. and the EU is in AAM's best interest (Oram, 2000). In response, AAM should register its Web site and privacy policy with U.S. Department of Commerce and one of the three U.S. organizations established to audit performance independently: TRUSTe, BBBOnline, or Secure Assure.

The following is a sample Internet privacy statement for use by AAM.com. Visitors would view the statement by clicking the "Privacy" link located at the bottom of the home page.

### AAM.com Privacy Statement

American Axle & Manufacturing, Inc. (AAM) is sensitive to privacy issues on the Internet. It is important that visitors to AAM.com know how AAM treats the information we collect about them on the Internet.

In general, visitors to AAM.com are anonymous and do not tell us their identity or any other information. AAM's Web servers only collect domain names and not the e-mail addresses of visitors. AAM aggregates this information and uses it to measure the number of visits, pages viewed, and average time spent on the site. Further, AAM uses the information to measure the use of the site and to improve site content.

However, it is necessary at times to obtain personal information, such as a visitor's name and address. When this occurs, the visitor is informed about how the information will be used. Normally, the information is requested to respond to a visitor's inquiry, process an order, or to allow access to specific account information. Visitor e-mail addresses are rarely made available to other organizations. When they are, visitors are offered the opportunity to limit distribution. In addition, visitors have access to view and edit any of their personal data collected on the site.

Information provided by a visitor to one of AAM's business units online is used to provide custom information about AAM's business support offerings. In addition, cookie technology may be employed to provide visitors with tailored information.

Cookie's are deposited on visitors' hard drives and allow AAM to recognize visitors when they return. Visitors that do not wish to receive cookies may set their browsers to notify them before receipt.

At times, AAM.com conducts online surveys to better understand the business needs of visitors. Whenever surveys are taken, AAM will let visitors know how the info will be used.

AAM.com contains links to other sites. While AAM tries to link only to sites that share our high standards for privacy, AAM is not responsible for the content or privacy practices of the other sites.

AAM.com is a S.A.F.E. (Secure Assure Faith Entrusted) Web site. The Secure Assure Organization regularly audits this site's compliance with the guidelines of the "safe harbor" agreement between the United States and the European Union.

### **Improvements to AAM.com's Existing Privacy Statement**

The following privacy statement is included among a variety of topics on the site's Legal Notices page (AAM, 2000):

"American Axle & Manufacturing, Inc., reserves the right to collect basic, generic information about visitors to this website, including: the site visited previous to this website; the time, date, and length of visitor's stay; pages viewed by visitor; and the visitor's internet service provider. This information is collected only for the purpose of helping us evaluate this website for activity and possible improvements and will not be used for any other purpose or otherwise disclosed by us. Any information provided by visitors through e-mail will be for our own use, or for the purpose specified in, or by the nature of, such communication, and may be shared with those of our employees, advisors, consultants, or contractors on such basis as we, in our sole discretion, determine appropriate, giving due consideration to the nature of such information. Any information which contains personally identifiable information such as your name, address, e-mail address, phone number, and the like will be kept confidential, and we shall respect any request to keep such information confidential. We shall treat any visitor questions or comments about this website, or any unsolicited correspondence received through e-mail or otherwise through this website, as non-confidential, and visitors providing such questions, comments, or unsolicited correspondence are advised to keep this in mind when transmitting such questions, comments, or unsolicited correspondence to us. American Axle & Manufacturing, Inc., reserves the right to amend this Privacy Policy at any time and without notice, except that any such revised Privacy Policy shall only apply to data collected after its effective date, and any revisions shall be posted at least ten days prior to the effective date."

The following is an improved version AAM.com's privacy statement.

Improvements are denoted by bracketed bold and italicized type.

“American Axle & Manufacturing, Inc., *[is sensitive to privacy issues on the Internet. It]* reserves the right to collect basic, generic information about visitors to this website *[Web site]*, including: ~~the site visited previous to this website~~; the time, date, and length of visitor's stay; pages viewed by visitor; and the visitor's internet service provider. This information is collected only for the purpose of helping us evaluate this website *[Web site]* for activity and possible improvements and will not be used for any other purpose ~~or~~ *[not]* otherwise disclosed by us. *[Cookie technology is employed to provide visitors with tailored information. Cookies are deposited on the visitors' hard drives and allow this Web site to recognize visitors when they return. Visitors that do not wish to receive cookies may set their browsers to notify them before receipt.]* Any information provided by visitors through e-mail will be for our own use, or for the purpose specified in, or by the nature of, such communication, and may be shared with those of our employees, advisors, consultants, or contractors on such basis as we, in our sole discretion, determine appropriate, giving due consideration to the nature of such information. Any information which contains personally identifiable information such as your name, address, e-mail address, phone number, and the like will be kept confidential, and we shall respect any request to keep such information confidential. *[In addition, visitors have access to view and edit any of their personal data collected by the site.]* We shall treat any visitor questions or comments about this website, or any unsolicited correspondence received through e-mail or otherwise through this website, as non-confidential, and visitors providing such questions, comments, or unsolicited correspondence are advised to keep this in mind when transmitting such questions, comments, or unsolicited correspondence to us. American Axle & Manufacturing, Inc., reserves the right to amend this Privacy Policy at any time and without notice, except that any such revised Privacy Policy shall only apply to data collected after its effective date, and any revisions shall be posted at least ten days prior to the effective date. *[AAM.com is a S.A.F.E. (Secure Assure Faith Entrusted) Web site. The Secure Assure Organization regularly audits this site's compliance with the guidelines of the “safe harbor” agreement between the United States and the European Union.]*”

After making the above changes to AAM's existing privacy statement, the policy now covers five of the most important characteristics of a well-written Web site privacy statement (Rotenberg, 1999). In its original form, the policy omitted a statement of corporate sensitivity to privacy, the company's use of cookie technology, and a provision to allow visitors to view and edit their personal data. In light of AAM's position as a global company, a statement ensuring compliance with recent “safe harbor” agreements

was included (Oram, 2000). In addition to the language improvements given above, the existing policy statement would be moved from the Legal Notices page to its own Privacy Statement page to ensure that it is easily found. Finally, a link, titled Privacy Statement, would be added to the bottom of AAM.com's home page.

### **Conclusion**

In conclusion, Web site privacy policies explain the responsibilities of the organization that is collecting personal information and the rights of the person who provided the information. Strong privacy practices give Web site visitors the assurance that personal information will not be misused. AAM's existing policy statement once modified and moved as detailed above will meet all the requirements of a properly crafted corporate Web site privacy policy statement (Rotenberg, 1999).

### **References**

- AAM. (2000). Legal Notices. *AAM.com*. <http://www.aam.com/legal.html>. Updated September 29, 2000. Accessed November 19, 2000.
- EPIC. (1997). Surfer Beware: Personal Privacy and the Internet. *Electronic Privacy Information Center*. <http://www.epic.org/reports/surfer-beware.html>. Updated June, 1997. Accessed November 24, 2000.
- Kane, T., & McEahern, M. (2000). Internet Privacy. *Anonymous.com*. <http://www.anonymous.com/study1.doc>. Updated April, 2000. Accessed November 24, 2000.
- Oram, A. (2000). Privacy Tectonics: The Shifting Responsibilities in the U.S. - European Data Protection. *Webreview.com*. <http://webreview.com/pace/print/2000/11/24/platformindependent/index.html>. Updated November 24, 2000. Accessed November 25, 2000.
- Rotenberg, M. (1999). Oversight Hearing on Electronic Communications Policy Disclosures. *Electronic Privacy Information Center*. [http://www.epic.org/privacy/internet/EPIC\\_testimony\\_599.html](http://www.epic.org/privacy/internet/EPIC_testimony_599.html). Updated May 27, 1999. Accessed November 24, 2000.

## Task 7

**Briefly, describe the points on which the U.S. and the EU agreed to resolve the long-standing data privacy rules dispute. Should the U.S. government adopt, in totality, the principles behind the European Commission Privacy Directive? Why or why not?**

The European Commission Privacy Directive requires member states to have extensive privacy protections (Smith, 2000). The directive demands that member states prohibit external transfers of data to countries without adequate protection. The European Union's (EU's) barring of such transfers could adversely affect global e-commerce.

The U.S. should not adopt, in totality, the principles behind the European Commission Privacy Directive. Many of the directive's rules were conceived more than a dozen years ago (Aaron, 2000). A time when there was no World Wide Web in Europe and mainframe computers were the norm. In light of today's distributed information networks, U.S. industry has made a strong case against application of the EU's privacy framework.

Adoption of similar principles in the U.S. would be expensive, impractical, and inflexible (Aaron, 2000). E-commerce companies in the U.S. have spent millions of dollars lobbying against privacy legislation. Personal data is a valuable commodity and e-commerce companies routinely seek, share, sell, and exploit it. Such information fuels the Internet and is a vital ingredient to new marketing technologies such as data mining and consumer profiling. In fact, the financial sector in the U.S. has undergone extensive consolidation so that it is able to share easily personal data between banks, brokerages, and insurance companies.

Recently, the U.S. and the EU agreed to resolve differences related to the EU's privacy framework (O'Harrow, 2000). The two sides agreed to a "safe harbor" data

privacy accord designed to enable U.S. companies, including financial institutions, to comply with European privacy regulations. The new agreement would allow the EU to certify that U.S. companies meet EU privacy guidelines. In order to meet the new safe harbor standards, U.S. companies are required to adopt the following standards:

1. Companies must tell visitors why they are collecting personal data and how they plan to use it - including whether it will be transferred to third parties.
2. Visitors have to agree in order for companies to share their personal data.
3. Unless the visitor has agreed otherwise, personal data can be sent only to third parties who have also agreed to these safeguards.
4. Companies must give visitors access to their personal data so that if the information is inaccurate, it can be corrected or deleted.

One point that the two sides have been unable to agree on is how to regulate data flows between financial institutions (Bloomberg, 2000). The Financial Organizations Act and politics surrounding the U.S. presidential election have been hampering agreement on this issue.

Finally, before the agreement becomes law, it needs approval from EU member states, on whose behalf the EU Internal Market commissioner negotiated (DeQuendre, 2000). In addition, the commission must obtain a nonbinding opinion from the European Parliament.

In conclusion, the “safe harbor” agreement between the U.S. and the EU is clearly a win for U.S. companies. The agreement continues to allow U.S. companies to collect data from people living in EU countries (Oram, 2000). In addition, the agreement only

addresses how a site's policy is enforced and not how that policy protects privacy.

### References

- Aaron, D. (2000, July 31). Profiting from privacy. *The Washington Post*, pp. OP-ED.
- Bloomberg. (2000). EU, U.S. Agree on Electronic Data Privacy. *Bloomberg News*.  
<http://news.cnet.com/news/0-1007-200-1571726.html>. Updated March 14, 2000.  
Accessed November 25, 2000.
- DeQuendre, N. (2000, June). Privacy agreement reached. *Security Management*, 44, 34.
- O'Harrow, R. (2000, June 1). U.S., EU agree on privacy standard; Accord removes barrier to trade. *The Washington Post*, pp. Financial.
- Oram, A. (2000). Privacy Tectonics: The Shifting Responsibilities in the U.S. - European Data Protection. *Webreview.com*.  
<http://webreview.com/pace/print/2000/11/24/platformindependent/index.html>.  
Updated November 24, 2000. Accessed November 25, 2000.
- Smith, J. (2000, March). Giving customers options: Opt in or opt out. *Beyond Computing*, 9.

## Task 8

### **What are the advantages of “universal service”; what are its drawbacks or implications?**

The 1996 Telecommunications Act charges the Federal Communications Commission (FCC) with the task of establishing policies to ensure universal access in the new Internet economy (IEEE, 2000). The law sets the goal of universal service for advanced telecommunications in all regions. Access to these services is addressed primarily in terms of making services available and “affordable” for schools, libraries, and health-care centers.

Historically, the term “universal service” has meant the availability of telephone service at a reasonable cost. Voice-grade communications has been the “service” in question. However, the 1996 law no longer confined the definition of universal service to traditional telephone service (Mueller, 1997). Universal service became an “evolving level of telecommunication services.”

The definition was also required to take into account advances in telecommunications and information technology. The FCC must now include any telecommunications service subscribed to by a majority of residential customers. In addition, the FCC must update the definition periodically. Once a service becomes part of the universal service definition, it is eligible for subsidy supports.

### **Advantages**

There are clear social and economic benefits that result from connecting all Americans (Cooper, 1996). These benefits include improved education, enhanced access to health care services, and better paying jobs. Universal service, as mandated by the 1996 law, provides geographic equality in the provision of advanced services. All

consumers, including those with low incomes living in rural, high-cost areas, would have access to services at rates that are “reasonably comparable” to those available in urban areas (Mueller, 1997).

Another advantage of universal service is that the availability of service on a universal basis makes it possible for our social system to function more efficiently (Sawhney, 1994). For example, in the case of the nationwide telephone network, each additional subscriber increases the value of the entire network. This is because millions of other subscribers are able to access the new subscribers.

### **Drawbacks**

Since the 1996 law mandates the equal availability of advanced services, one implication is the negative effect it could have on the introduction of new services by common carriers (Mueller, 1997). If the FCC mandates that service must be simultaneously available in all markets regardless of size or demand, suppliers may be unwilling to deploy new technologies in any market. In fact, innovations are unlikely to attract investors if they must compete with subsidized existing technologies (Gasman, 1998).

While government mandated and cross-subsidized universal service would lead to equality, it could also lead to bigger companies, less competition, and fewer opportunities for innovation (Browning, 1994). The FCC’s efforts to introduce competition into telecommunications markets are incompatible with the concept of universal service. Attempting to mix the two, competition and universal service, could result in anemic markets that are regulated more for the benefit of business interests than for consumers.

Past efforts to implement universal service (i.e. government created monopolies

whose profits were used to cross-subsidize) have not worked (Metcalf, 2000). The Internet revealed proof of this failure. While computer-processing power is millions of times faster than it was just a few years ago, the fastest connection available to most consumers is a 56K dial-up modem. In fact, Grove's law states that bandwidth doubles every 100 years. This is the result of past efforts by the government to legislate universal (i.e. substandard) service.

### **Conclusion**

In conclusion, the drawbacks of universal service outweigh its benefits. New technologies and networks require a shift toward regulation that promotes open access and not universal service (Browning, 1994). Regulation focused on universal service requires the FCC to decide what services people should have and the price they should pay for them. In contrast, open access protects the ability of people to make their own choices.

### **References**

- Browning, J. (1994). Universal Service - An Idea Whose Time is Past. *Wired Digital*. [http://www.wired.com/wired/archive/2.09/universal.access\\_pr.html](http://www.wired.com/wired/archive/2.09/universal.access_pr.html). Updated September, 1994. Accessed November 25, 2000.
- Cooper, M. (1996). Universal Service: A Historical Perspective and Policies for the Twenty-First Century. *Benton Foundation*. <http://www.benton.org/Library/Prospects/prospects.html>. Updated December 9, 1996. Accessed November 25, 2000.
- Gasman, L. (1998). Universal Service: The New Telecommunications Entitlements and Taxes. *Cato Institute*. <http://www.cato.org/pubs/pas/pa-310.html>. Updated June 25, 1998. Accessed November 25, 2000.
- IEEE. (2000). IEEE-USA Position Statement on Universal Access. *Institute of Electrical and Electronics Engineers*. <http://www.ieeeusa.org/forum/POSITIONS/unaccess.html>. Updated November 6, 2000. Accessed November 25, 2000.

Metcalf, B. (2000). What's Wrong with the Internet: It's the Economy, Stupid. *IEEE*.  
<http://computer.org/Internet/v1/metcalfe9702.htm>. Updated February, 1997.  
Accessed November 25, 2000.

Mueller, M. (1997). Myth made law. *Communications of the ACM*, 40(3), 39-46.

Sawhney, H. (1994). Universal service: Prosaic motives and great ideas. *Journal of Broadcasting and Electronic Media*, 38(4), 375-395.

## Task 9

**Is the Digital Divide a legitimate concern in the U.S. or merely an outgrowth of partisan politics? What role should the U.S. government play in bridging the so-called “digital divide”? How serious is the “digital divide”, internationally? Give examples.**

The term “digital divide” was coined in a 1997 U.S. Commerce Department report to describe the barriers to Internet access faced by low-income citizens (Williams, 2000). Since then, the term has evolved to refer to the gap between the Web-enabled and those with access to only the traditional economy.

### **Legitimate Concern?**

Those concerned about the digital divide point to the fact that citizens without Internet access have less opportunity to take part in the new information-based economy. For example, there is less opportunity for these individuals to take part in education, training, entertainment, shopping, and communications opportunities. Poor citizens, living in rural areas, are 20 times more likely to be left behind than are wealthier citizens living in urban areas.

Another concern is that although Internet access among minorities is growing at a faster pace than the national average, it is still not fast enough to prevent the digital divide from widening (Abramson, 2000). For example, the gap between African American Internet usage and national usage grew three percentage points between December 1998 and August 2000. Similarly, the gap between Hispanic households and the national average grew four percentage points during that same period.

### **Partisan Politics?**

In contrast to the above, others see the digital divide as an outgrowth of partisan politics (Frezza, 1999). They point out that while the gap between poor black and

Hispanic households has grown this should not overshadow the fact that during the same period Internet usage increased 50 percent across the board. At that rate, it is not difficult to figure out how long it will take until the whole nation is fully wired. Many view the digital divide as a false alarm sounded by Democrats because an important constituency (poor blacks and Hispanics) are construed to be “losing ground.”

### **Role of the Government**

Few innovations have been adopted as rapidly as the Internet – not the telephone, electricity, television, or indoor plumbing. Growth of the Internet has been fueled by drastic decreases in computer prices and a lack of government intervention (Frezza, 1999). At the Internet’s current growth rate, increased computer production volumes will lead to even lower computer prices. In fact, Internet access is cheaper than a cigarette habit and well within the reach of most Americans.

In light of the above, the government’s role in the issue should be minimal and take the form of limited tax breaks to companies that provide technology and training to low-income communities and schools (Brandt, 2000). This is more efficient and effective than paying extra taxes for the government to add Web-connected computers to schools.

### **International Divide**

While there is considerable debate about the U.S. digital divide in technology access, the real gap lies between the U.S. and the rest of the world (Editor, 2000). Moreover, one-third of the Earth’s population has no electricity. For example, Nepal, whose landlocked position at the top of the world helped protect it from invaders, is now looking to information technology to decrease its isolation. This will prove to be a monumental task in a country with only a 39 percent literacy rate and 75 percent of all

households without electricity (Goodman, Kelly, Minges, & Press, 2000).

Research conducted late last year found that rich countries are increasing their use of IT by 23 percent annually (Wilson, 2000). In contrast, developing nations grew by only 18 percent. This substantial five-point gap is continuing to widen. The implications for international trade and global economic expansion are troublesome. In addition to the challenges presented by a lack of infrastructure, third-world resistance to e-commerce also increases the global digital divide (McCullough, 2000). While industrialized regions such as North America and Europe accelerate the global e-commerce boom, India still requires manual dots for trade clearance.

### **Conclusion**

Internet access among all Americans is growing at a staggering rate. At the current 58 percent growth rate (from December 1998 to August 2000), the whole issue of a digital divide will become mute as the majority of poor and wealthy Americans surf the Internet (Abramson, 2000).

### **References**

- Abramson, R. (2000). Report: Digital Divide Widens. *The Standard*.  
<http://www.thestandard.com/article/display/0,1151,19429,00.html>. Updated October 16, 2000. Accessed October 21, 2000.
- Brandt, R. (2000). Bridging the Digital Divide. *UpsideToday*.  
<http://www.upside.com/texis/mvm/print-it?id=38d82fa20&t=/texis/mvm/news/news>. Updated April 11, 2000. Accessed November 5, 2000.
- Editor. (2000, November 23). Gratitude for a great nation. *Tampa Tribune*, pp. 26.
- Frezza, B. (1999). Clinton-Gore's Digital Divide: Race Mongering on the Internet. *InternetWeek*. <http://www.internetwk.com/columns/frezz080299.htm>. Updated August 2, 1999. Accessed November 26, 2000.
- Goodman, S., Kelly, T., Minges, M., & Press, L. (2000). Computing at the top of the

world. *Communications of the ACM*, 43(11), 23.

McCullough, S. (2000, October). Delivering the global goods. *Manufacturing Systems*, 18, 56.

Williams, S. (2000). Upshot: Should Government Solve the Digital Divide? *UpsideToday*. <http://www.upside.com/texis/mvm/print-it?id=38fb48c30&t=/texis/mvm/news/news>. Updated April 18, 2000. Accessed November 5, 2000.

Wilson, E. (2000, September 4). Take next steps to narrow the global IT gulf. *Computerworld*, 34, 33.