MIT Privacy Protection of Job Applicant and Employee Information

6.805

December 14th, 2005

Jacqueline Tio

"MIT, MIT, let me in…" --- "Not by the hair of my chinny chin chin..."

INTRODUCTION

He huffed, and he puffed, and he blew the house down. Such were the fabled actions taken against the pig who did not build a house out of bricks. These actions may also be taken against those who ignore the full implications of the Internet and its effect on the privacy of job applicant and employee information. The Internet has not only created new modes of information access, but has also prompted rapid shifts toward using web-based systems and electronic databases to collect, process, and store job applicant and employee information. If these changes occur too carelessly, however, the unchecked dangers resulting from identity theft, information sharing, and fraud may create a gale force too mighty for these information systems to handle.

The technology and policies in place for job applicants and employees at MIT provide a solid case study for determining the credibility of these concerns. Currently, almost all transactions involving employee information are in some way connected to the Internet. Job applicant and employee information are funneled through web-based systems such as Webhire and SAPweb. In-house processing of information in the Human Resources Department (HR) and Information Services and Technology (IS&T) also rely heavily on electronic communication. A review of MIT systems and of the policies of MIT, Harvard, the European Union, the United States, commercial job databases, and Hewlett Packard indicates that the current house safeguarding job applicant and employee information at MIT needs renovation. A set of recommendations based on this review proposes that privacy cannot be adequately protected unless significant measures are taken to change MIT policies. This includes explicitly protecting job applicant information, setting minimum standards for the electronic handling of job applicant and employee information, and increasing awareness among job applicants and employees of the fate and distribution of these types of information. Unless these recommendations are taken seriously, at present, MIT may have its bricks, but it still lacks the mortar needed to build a house that adequately safeguards both job applicant and employee information.

THE STAKES

Privacy Concerns of Job Applicant and Employee Information

Numerous resume databases have made it easier than ever to search and apply for jobs. At the same time, the privacy of information posted online has become more vulnerable to both fraudulent and criminal behavior. Applicant information gleaned from resumes can be particularly invasive because of the types of information it provides such as home addresses, social security numbers, telephone numbers, and educational background. According to Pam Dixon, the executive director of the World Privacy Forum, resumes of mid-career professionals are particularly attractive to identity thieves because of the depth of information they provide. Some criminals have even gone so far as to post fake job positions online to solicit more personal information from their victims.[1] Others have infiltrated job databases and amassed as much as 20,000 resumes before any red flags were raised.[2] Although no case of job applicant information leakage has made headlines at MIT, the implications of these cases are chilling: a supply and demand for job applicant information has cultured a new black market, and the Internet in all its glory has empowered criminals to enter it with little or no detection.

Compounding privacy concerns of job applicant information are that of employee information. In this regard, MIT has faced its own crisis with the accidental leakage of confidential employee information. In 2004, an MIT alumnus found the ID and social security numbers of over 11,000 MIT employees through Google. This information had accidentally been posted in a public directory for six months, and five employees suspected that they had been the victims of identity theft.[3] In January 2005, Harvard also faced an information leakage nightmare after realizing that confidential drug procurement and contact information of students and employees were accessible through a loop-hole in the PharmaCare website. It is unclear whether this breach of protected information violated federal law, but concern arose over the potential violation of the Family Educational Rights and Privacy Act (FERPA), which grants certain students security protection, and the Health Insurance Portability and Accountability Act

[1] "Online Resumes Turn Risky." San Francisco Chronicle. 4 July 2005.
[2] Dixon, Pam. "Resume Database Nightmare: Job Seeker Privacy at Risk." Privacy Rights Clearinghouse. 19 February 2003. Online. 11 November 2005. Available: http://www.privacyrights.org/ar/Dixon-JobPrivacyRpt.htm
[3] Lugovskaya, Tatyana. "MIT Employees' Social Security Numbers Found in Public File." The Tech. 16 April 2004. Online. Available: http://www-tech.mit.edu/V124/N20/20ssn.20n.html

(HIPAA), which protects medical information. Although only the latter would apply to employee information, this incident suggests that the lack of protection of employee information is as dependent on general information practices as it is on employee information practices.[4]

Thus far, however, MIT and Harvard should count themselves lucky. At least the problems were accidental and investigative, not deliberate. Just this year in the course of only a few weeks, confidential information of roughly 180,000 people from Berkeley, Northwestern, and California State University were purposely breached by hackers and thieves.[5] In light of this trend, the privacy of job applicant and employee information at MIT deserves a thorough review before an even bigger, meaner wolf decides to come and blow our house down.

Electronic Information inside the House

Since the mid-1970s, the MIT Human Resources department has been using electronic databases to store employee information. Today, the reliance on technology has progressed to the point where almost all campus employee information is handled electronically. Even resumes and documents submitted in paper form are scanned into electronic form by means of an electronic imaging system. Because of the reliance on electronic databases to enter, maintain, and update employee information, the HR department has established a closely working relationship with different departments and vendors to maintain employee information. This includes working with other parts of the Institute, such as Information Services and Technology, and contracting out to external vendors to maintain databases.[6]

Electronically storing information through the Internet, however, increases vulnerability to theft by faceless thieves. Web-based systems, such as Webhire and SAPweb, now maintain job applicant and employee information. Employee transactions, for instance, depend on filling out HTML forms and sending it to a general mailing list. In-house processing of documents, memorandums, and paperwork also rely extensively on the Internet through the use of electronic mail.[7] A review of Webhire, SAPweb, and in-house processing of information reveals that the

---

[4] Russel, J. H; Theodore, E.S. "Drug Records, Confidential Data Vulnerable." The Harvard Crimson. 1 January 2005. Online. Available: http://www.thecrimson.harvard.edu/printerfriendly.aspx?ref=505402
[5] Zeller, Jr., Tom. "Some Colleges Falling Short in Security of Computers." New York Times. 4 April 2005.
[6] Correspondence with Claire Paulding, Senior Manager of Human Resources Information Services. 16 November 2005.
[7] Paulding, Claire, Senior Manager of HRIS. Interview. 18 November 2005.

threats to privacy continue to exist in the use of these web-based systems and in the lack of detailed policies regarding the distribution of these types of information.

BRICKS WITH NO MORTAR

Webhire

Around 1993, the HR department began to use Restrac, an earlier version of Webhire, as a means to process and track job applicant data electronically.[8] In the summer of 2000, an Applicant Tracking Team was assigned to review this applicant tracking system for future adoption on a larger scale. Although acknowledging, but not going into further detail, that disadvantages of using Webhire included its lack of security, the team decided that these disadvantages were outweighed by the needs of hiring managers who were receiving insufficient support in the recruitment process. Ultimately, the team endorsed Webhire but flagged several policy issues for consideration such as the definition of an actual job applicant, the use of information from job applicant pools, and the lifetime of a resume in a job applicant pool.[9]

In January 2002, the Restrac applicant tracking system was formally upgraded to Webhire, accessible online through Staffing Services on the HR website.[10] Through Webhire, resumes and job applicant data are now collected and stored off-campus. Information from this database is made available to the HR department, which houses its own recruiting office trained to work with the Webhire system. In transferring data, moreover, Webhire uses Secure Sockets Layer (SSL) software to encrypt transactions between their database and an end user's web browser.[11]

The upgrade to Webhire was characterized as an advantageous move that allowed instantaneous access to resumes and applications, improved database searching capabilities, and improved ability to track Equal Employment Opportunity and Affirmative Action Program

---

[8] Correspondence with Wendy Williams, Director of HR Staffing Services. 30 November 2005.
[9] Applicant Tracking Team Final Report. HR Department. July 2002. Online. Available: http://web.mit.edu/ist/delivery/hrpayroll/pdf/finalrpt_aptrack.pdf
[10] Williams, Wendy. Staffing Services, Report to the President 2002-2003. Online. Available: http://web.mit.edu/annualreports/pres03/
[11] "Webhire Recruiter Architecture and Security." Webhire. 2 December 2005. Document acquired from Webhire Representative.

information.[12] These advantages, however, should not obscure the threats to privacy that linger in its shadow. When a job applicant applies online, the information is either automatically sent by e-mail to the hiring manager, automatically sent by e-mail to the hiring manager after a pre-screening process, reviewed by Staffing Services, or reviewed by a Data Link Control (DLC) HR representative who then sends it by e-mail to a hiring manager. When the Webhire system transfers information through email, it uses SSL encryption to protect the transmitted information.[13] The problem, however, may arise in the transfer of information within MIT once it is received from Webhire. Although some MIT employees may be protected from interception of their e-mails with SSL enabled secure outbound SMTP authentication, the use of SSL to encrypt sent messages is not required. The use of e-mail to transfer data without SSL encryption, therefore, occurs at the risk of having this information stolen by a clever thief or perhaps by an even cleverer computer virus.

Privacy is also threatened by the electronic storage of information. The application procedures on the Staffing Services website state that "the system [WebHire] allows us to store the resumes we receive in a searchable database so you may be considered for any position where there might be a match between the requirements of the job and your qualifications.[14]" This pool of job applicant information grows bigger everyday. The HR department currently has on hand four years of job applicant data, and each year the pool increases by roughly 32,000 resumes. Although the HR department has considered archiving older data, there has been no mention of deleting it. By request, Staffing Services can delete a job applicant's information. However, few, if any, job applicants are aware that their information is still stored in MIT's database.[15]

Job applicants, thus, are preemptively handicapped from protecting their privacy. Although MIT states that job applications are stored in a searchable database, they give job applicants no choice for opting out and give no warning to job applicants that their information is stored indefinitely.

Finally, although the HR department works hard to ensure the confidentiality of job applicant information, when job applicant data is sent to a hiring manager, the confidentiality of

---

[12] Williams, *op. cit*. 8.
[13] Correspondence with Webhire Technical Support. 8 December 2005.
[14] Staffing Services. "Job Search for External Candidates." Human Resources at MIT. Online. Internet. 21 November 2005. Available: http://sh.webhire.com/Public/631/
[15] Williams, *op. cit.* 8.

that information is passed into the hands of the department of that hiring manager.[16] HR has no oversight mechanism to ensure the confidentiality of information past this point, and the computers in these departments are not held to any minimum security standard.

SAPWeb and SAP R/3

Apart from the system used to handle job applicant information, a separate system exists to handle employee information. In 2001, MIT Human Resources began to use the SAPweb Self-Service system that allowed employees to select their benefit options. Over the next few years, SAPweb Self-Service grew into a system that is now used by employees and by Data Link Control (DLC) administrators to maintain employee information. SAPweb operates as the front-end web interface of the SAP R/3 system, where employee information is actually stored.[17] SAP R/3 is MIT's financial system of record that was adopted in 1996. This system houses an enormous amount of information and is maintained by IS&T.[18]

The flow of employee information through SAPweb is protected by MIT personal certificates. No employee information is sent through e-mail. Instead, a Hypertest Transfer Protocol over Secure Socket Later (HTTP over SSL) is used in communicating between users' web browsers and SAPweb. Moreover, all communications between the SAP web-server, the SAP Internet Transaction Server, and SAP R/3 are protected by a network that uses MIT Kerberos credentials. All transactions are also recorded by a log that tracks any changes made to employee information. Information updates and changes within SAPweb, therefore, are relatively secure and can be tracked.

Access to SAP R/3 through SAPweb is usually given to all administrative officers and personal administrators. It is also granted through departmental authorizations that are distributed separately for education data, emergency contact information, ethnic and military information, and telephone directory information. The employee information available to any department, however, is limited to employees of that department. To track this hierarchy of information access, a separate database is used to monitor and to control access to employee

[16] Ibid.
[17] Correspondence with Diana Hughes. IS&T Communications Administrator. 1 December 2005.
[18] "Implementation History." SAP for MIT. Online. 1 December 2005. Available: http://web.mit.edu/sapr3/history.html

information.[19] Although information stored in SAP R/3 can be distributed outside of HR and IS&T departments, no oversight or standard guidelines currently exist to manage the handling of information once it is retrieved from SAP.

Finally, similar to Webhire, SAP R/3 has never deleted any employee information. Currently, MIT has approximately 10,000 employees, all who have at least home or work addresses stored in SAP R/3.[20] Although this information is stored in SAP R/3 and not formally transmitted through e-mail as in Webhire, the information pool continues to grow, and the potential for accidentally leaking an increasing larger pool of information remains an ever present danger for HR and IS&T.

Pervasive Privacy Concerns

Even with the most secure Webhire and SAP systems, there is still a significant threat to privacy that arises from normal, human behavior. According to Jeff Schiller, the network manager for MIT, the problem is not "mail in flight," but "data at rest.[21]" Policies that too severely lockdown access to information trigger a splatter effect. When employees finally receive requested confidential information, they often leave it on their desktops to avoid having to go through the tortuous process of acquiring that information again. The splatter effect occurs when they share this information by e-mail with other colleagues who are looking for quick and easy access. Given that most employees use an SSL enabled secure outbound SMTP authentication to protect their e-mail, the security problems arise not with data transmission but with data storage on desktop computers that are currently subject to no security requirements. Information can be easily extracted from desktops that lack the necessary software and encryption packages to protect stored confidential information from unauthorized access. At present, no policy exists to require the use of such a package, but considerations for creating a desktop encryption package are on the table.

Another pervasive concern in the handling of job applicant and employee information is the lack of training, education, and understanding of technology that characterize some employees who routinely use and transfer confidential information. Indeed, some employees

[19] Hughes, *op. cit.*
[20] Ibid.
[21] Schiller, Jeff. Interview, MIT Network Manager. 1 December 2005.

may *unknowingly* transfer confidential data through e-mail on a routine basis. In one instance, an employee sent a DAT file attachment to another employee without realizing that in addition to the three fields of information that were being used for the task at hand, roughly 100 MB of additional personal information was also contained in that file. Viruses have also been found to be capable of extracting random files, some of which have been confidential, and transferring them to others through e-mail.[22] Although the destination of confidential information may seem secure, the carelessness in sending hidden confidential information imposes an unnecessary risk on employee privacy and an unnecessary liability risk on MIT.

The carelessness of using confidential information also raises another issue: the unnecessary use of certain confidential information for identification purposes. Social security numbers, for instance, do not need to be used if there is no statutory information. Yet before the 2004 incident at MIT, they had been used internally within the HR department in some employee identification practices that did not require the use of social security numbers.[23] Since the 2004 incident, the HR department has begun to use MIT ID numbers in lieu of social security numbers to identify employees.[24] Although the unnecessary use of confidential information has been mitigated, in the absence of a formal institute-wide policy encouraging this practice, the use of confidential information by other departments who receive information from the HR department remains to be a black-box.

MIT POLICIES ON INFORMATION AND PROTECTION OF PRIVACY

Many of the problems that arise in the handling of job applicant and employee information can be alleviated through changes in MIT policy. Since the 2004 incident, there have been no official policy changes to MIT Policies and Procedures or the HR Personnel Manual with regard to the handling of confidential information.

[22] Ibid.
[23] Ibid.
[24] Paulding, *op. cit.* 7.

Policies Concerning Job Applicant Information

The beginning of MIT Policy on Privacy of Information (Section 11.2 of MIT Policies and Procedures) states:

"Recognizing that specific items of information about current (as well as former) individual students, faculty, and staff must be maintained for educational, research, and other institutional purposes, it is MIT policy that such information be collected, maintained, and used by the Institute only for appropriate, necessary, and clearly defined purposes, and that such information be controlled and safeguarded in order to ensure the protection of personal privacy to the extent permitted by law. [25]"

This statement specifically addresses student, faculty, and staff, but makes no mention of a job applicant. This, therefore, has implications in other parts of MIT policy that use this definition. For instance, MIT Policy on the Use of Information Technology (Section 13.2.2) states:

"Individuals who manage or use the information and computing resources required by the Institute to carry out its mission must protect them from unauthorized modification, disclosure, and destruction… Protection shall be commensurate with the risk of exposure and with the value of the information and of the computing resources."

According to this policy, individuals managing or using information are required to protect that information, yet the level of protection is measured by the risk of exposure and value of the information. Since the value of job applicant information is not explicitly stated, this at most implies minimal levels of protection for job applicant data, if any. Additionally, in light of the increasing number of job applications processed through the web, the federal government, which requires tracking race, national origin, and gender for all job applicants, has already issued new guidelines defining a job applicant.[26] MIT actually uses job applicant data to meet these

[25] MIT Policy and Procedures. 1997. Online. 15 November 2005. Available: http://web.mit.edu/policies/index.html
[26] Pitney Hardin LLP. "EEOC Guidelines Require Tracking Some Internet Applicants." *New Jersey Employment Law Letter*. April 2004. Online. Lexis-nexis.

requirements, but despite cooperating with the federal government's efforts to adapt to the effects of web-based job databases, it has taken no moves toward protecting the privacy of such information through policy.

Policies Concerning Employee Information

Informally, MIT policies concerning employee information within the HR department have changed since the information leak in 2004. Instead of using social security numbers, MIT ID numbers are now used to identify employees.[27] Formal policies, however, have not changed. This includes MIT Policies and Procedures (Sections 11.1, 11.2, 13.2, 13.3, 13.4) and the Human Resources Personnel Manual.

Although a listing of protected employee information is not explicitly given, MIT Policy on Privacy of Information (Section 11.2) does give a listing of unprotected, standard personnel information, such as MIT employment, job title, department, and telephone number. This implies that information not on this list is considered protected and cannot be released without individual consent or a court order and/or legal process. This definition of protected information is taken seriously by those in the HR department who consider information not listed to be protected.[28] This, however, does not guarantee that a uniform definition of confidential information has been agreed upon throughout the department or even the institute.

In addition, the flavor of the words MIT uses in advising people to handle confidential information is passive rather than active. For example, MIT Policy on Privacy of Information (Section 11.2) states:

"Persons with responsibility for records containing personal information should exercise care to ensure accuracy and completeness. Safeguards *should* be provided to protect personal information against accidental or intentional misuse or improper disclosure within or outside MIT."

[27] Paulding, *op. cit.* 7.
[28] Paulding, *op. cit.* 7.

This section advises people handling confidential information to use safeguards to protect against accidental or intentional misuse of personal information.[29] The operative word, however, is *should* rather than *must*, and the overall policy does not mandate that necessary security measures be taken in handling confidential information. To be fair, the word *must* does surface in MIT Policy on the Use of Information Technology (Section 13.2), which states:

"The privacy of individuals *must* be protected, regardless of the form or the location in which the information about them is stored, including computer media. Access to personal information *must* be limited to authorized users for approved purposes. Such information *must* be safeguarded from unauthorized access. [30]"

Although stronger language is used in mandating the existence of safeguards to protect personal information, the definition of a safeguard is left open-ended. The level and types of safeguards are not specified and, therefore, may vary from department to department.

The HR Personnel Manual also describes using and collecting employee information. It specifically outlines the duties of the HR Department to maintain employee records and outlines the information that is kept within each employee record, the people that can access these records, and how changes in these records are to be made.[31] The manual, however, provides no additional guidance on the handling or storing of such information once it is in the hands of an authorized user. Similar to the policy on the use of information technology, the electronic means by which confidential information is handled is left to the discretion of each individual accessing that information.

HARVARD POLICIES ON INFORMATION AND PROTECTION OF PRIVACY

To provide a basis of comparison, Harvard's policies concerning the protection of job applicant and employee information was also evaluated. A brief overview of the architecture of its job applicant and employee information systems is provided in the Appendix.

[29] MIT Policies and Procedures, *op. cit.*
[30] Ibid.
[31] "HR Personnel Policy Manual." MIT Human Resources. Online. 2005. http://web.mit.edu/hr/policy/1-1.html

Policies on Job Applicant Information

Harvard policy on information security and privacy of confidential data addresses the same issues outlined in MIT Policies and Procedures on the protection of privacy and use of information technology.[32] Similar to MIT, it does not explicitly mention the protection of job applicant information. Job applicant information submitted to Harvard is collected through a web-based system known as HIRES. According to the job application website, resumes of outside job applicants are also eventually merged into a larger searchable database. The privacy of job applicant information, therefore, is a valid consideration. Yet Harvard policy only stresses the importance of protecting "confidential data," which is defined as "personally identifiable information about Harvard people (from core Harvard databases)…[33]" Job applicants, presumably not yet Harvard people, are not included in this definition, and privacy policies afford little, if any protection to them.

Policies Concerning Employee Information

Employee information, in contrast to job applicant information, does fall into the definition of confidential data which is protected by Harvard policy. Moreover, its policy on information security and privacy of confidential data is much more specific than that of MIT. Harvard requires confidential data to be encrypted when transferred. It requires employees who access confidential data to sign a confidentiality agreement. It requires all data network computers to be up-to-date on security patches and to follow "normal good computer security practices." It also requires outside vendors who handle its confidential data to sign a contract agreeing to protect confidential data before doing work for the university.[34]

Similar to MIT, however, several other key policies remain passive rather than active. For instance, the Harvard policy on Information Security and Privacy states:

[32] "Harvard University Information Security and Privacy." Online. 2005. Available: http://www.security.harvard.edu/tech_security/
[33] Ibid.
[34] Ibid.

"Confidential Data stored on an individual's personal computer at Harvard *should* be encrypted. Confidential Data stored on a laptop computer, or any personal computer not located at Harvard *must* be encrypted."

Similarly, for target computers most vulnerable to security breaches, Harvard policy states:

"Access to these computers *should* be limited to local console access or authenticated and encrypted network-based access.

The use of smart cards for user authentication of system administrators is *encouraged* where computers contain particularly sensitive information or provide core university services.[35]"

The first policy differentiates between using the word *should* and *must* for encryption practices on-campus and off-campus. Curiously, for desktop storage of sensitive information on-campus, the policy takes the passive stance. The use of the words *should* and *encourage* in the latter policy indicates that though Harvard may be keen on protecting information in flight, its policy is still weak at the seams for information in storage. The real vulnerabilities, such as information stored on desktops that are subject to unauthorized access, are protected through guidelines rather than requirements. Yet in years past, e-mail privacy violations reported to the Dean of Harvard College primarily consisted of internal problems concerning information in storage not external, technical problems concerning information in flight. These internal problems involved behavioral issues of handling stored information, such as the sharing of passwords.[36] Despite the apparent contradiction between policy and reality, however, at least Harvard has formally provided more specific warnings where MIT has not, such as warnings about potential problems and security issues that need to be considered in handling confidential data through computer-based technology.

Harvard's Personnel Manual is also more detailed and extensive than MIT's Personnel Manual in the handling of confidential information. Not only are different levels of confidential

[35] Ibid.
[36] Lewis, Harry R. Phone Interview by Jacqueline Tio. 6 December 2005.

information and distribution described, but a detailed guideline of how this information should be accessed by those who are authorized to access it is also provided under a heavy note of caution. The manual also explicitly states an expectation of employees to use the "current best practices" in maintaining the security of their computer systems and lists ways to meet this guideline, such as using anti-virus software, ensuring remote access network security, handling junk mail, and listening to various directives issued by the department or other parts of the institute. Curiously, access to this personnel manual is protected by Harvard PIN authentication whereas MIT offers open access to its HR Personnel Manual.

UNITED STATES POLICY IN RELATION TO EUROPE

Outside of MIT or Harvard, a complex network of federal and state law requires employee record-keeping for employees under laws such as wage and hour law, equal opportunity employment law, and occupational safety and health law. The Occupational Safety and Health Act, for instance, mandates that employers keep employee medical records for thirty years past the period of an employee's employment. Very little federal legislation, however, actually exists to protect the privacy of this employee information. Under U.S. law, employer computerized record-keeping and electronically stored employee information are not treated any differently from paper record-keeping. The only distinction with regard to electronic information is made in Section 2702 of the Electronic Communications Privacy Act which "prohibits an entity providing electronic communication service to the public from divulging the contents of a communication while in electronic storage or, for a provider of remote computing services to the public, from divulging the contents of any communication carried on the service, subject to express exceptions." This, however, does not address privacy issues for electronic databases that are not connected to electronic communications. Additionally, there is no specific reference to employee records. Only a handful of states, such as Massachusetts and California, have taken steps toward directly protecting privacy through state laws or charters, but even these are generic.[37] Massachusetts's law, for instance, states that "…a person shall have a right against

[37] Finkin, Matthew W. "Information Technology and Workers' Privacy." 23 Comp. Lab. L. & Pol'y l 471 (2002). Lexis-nexis.

unreasonable, substantial or serious interference with his privacy.[38]" The shape and form of privacy remains unspecified and open to interpretation.

Only employee information related to disability or health information is currently protected under U.S. law under the American Disabilities Act (ADA) and HIPAA. This stands in stark contrast to the stance taken by the European Union on the privacy of personally identifiable information. In the mid-1990s, the EU closely analyzed the implications of technology on privacy, a right that is viewed as fundamental. Through the EU Privacy Directive of 1995, EU member states comprehensively and proactively adopted measures to protect electronic employee information, specifically described as being processed entirely or in part through automatic means. Through this directive, employees now have the rights to be informed about information collecting methods, to access and correct their personal information, and in special circumstances to prohibit the collection of their information.[39]

In addition, European personal data collection companies must post privacy policies, give reasons for data collection, allow customers to review and change data, allow customers to opt out of information collection, disclose with whom the data will be shared, protect the data with security measures, and restrict information sharing to countries that have adopted similar policies.[40] The list may seem long, but the reality has proven that such specifications can be feasibly met regarding the use of personal information.

LEGAL IMPLICATIONS FOR PRIVACY VIOLATIONS

MIT Liability for Privacy Violations

Although the U.S. does not have much legislation protecting job applicant or employee information, it does have laws regarding employer liability for crimes committed by its employees. The progress made in computer technology has been accompanied by an increase in internet crimes that have significant implications on employer liability for injuries from crimes

[38] General Law of Massachusetts. "Chapter 214: Section 1B Right of Privacy." Online. 2005. Available: http://www.mass.gov/legis/laws/mgl/214-1b.htm
[39] Lasprogata, G; King, N.J.; Pillay, S. "Regulation of Electronic Employee Monitoring." 2004 *Stan. Tech. L. Rev.* 4 (2004). Lexis-nexis.
[40] Kohel, Matthew. "Australian Government's Substandard to Attempt to Allay Privacy concerns and Regulate Internet Privacy in the Private Sector." 27 Brooklyn J. Int'l L. 703 (2002). Lexis-nexis.

and wrongful acts committed by its employees.[41] This implies that for any breach of privacy under laws such as the ADA, HIPAA, and FERPA, MIT may be held liable in the court of law.

As early as 1909, the United States Supreme Court ruled that a company can be held criminally liable for the acts of their employees that occur under the authority conferred upon the employee by the company and that involve knowledge and purpose that are attributable to the corporation. In this case, the U.S. Supreme Court ruled that the Hudson River Railroad Company was held liable for the acts of its traffic manager, who had unlawfully regulated commerce by giving rebates to customers in order to encourage the use of Hudson River transportation services. Despite the railroad company's arguments that stockholders were being unfairly punished without due process, the Supreme Court charged that imposing such liability on the company was necessary to prevent the granting of a blanket immunity from punishment to any and all businesses involved in interstate commerce.[42]

Since this ruling, the standards used by courts to measure an employer's liability have included respondeat superior and negligent retention. According to respondeat superior, the employer is held liable for any wrongful action of its employee if the act occurred within the "scope of the employment"or if it was foreseeable by the employer. The "scope of employment" has been defined as conduct that is the kind an employee is employed to perform, that occurs within authorized time and space limits, that occurs in some part to serve the employer, and, in cases where force was used, could have been foreseeable by the employer. According to negligent retention, an employer who puts an "unfit person in an employment situation involving an unreasonable risk of harm to others" is held responsible for the actions of that employee. Relevant court cases have continued to expand employer liability in a number of instances, ranging from securities fraud to sex-related crimes to wrongful deaths. If a company provides employees with the electronic means to commit egregious crimes, clear policies must be iterated to minimize the risks of criminal or wrongful act liability that accompany computer technology.[43] For MIT, this implies that empowering employees with the means to invade or expose thousands of people's privacy places a responsibility on MIT to protect this information

[41] Davis, Erin M. "The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed by Their Employees." 12 Alb. L.J. Sci. & Tech. 683 (2002). Lexis-nexis.
[42] *New York Cent. & H. R.R. Co.* v. U.S., 212 U.S. 481 (1909)
[43] Davis, *op. cit*.

if not out of concern for its job applicants and employees, then out of concern for a potentially expensive liability suit in the court of law.

Expectation of Privacy for E-mail

The legal opinion on the privacy of employees' e-mail messages may also affect the privacy of job applicant and employee information that are transferred through e-mail. Several court decisions have repeatedly ruled that employees have no reasonable expectation of privacy to contents in their e-mail. In one case, two employees were fired after investigation into a sexual harassment complaint that uncovered inappropriate e-mail messages. The employees charged that the investigation of their e-mail messages by their employer had wrongfully invaded their privacy and violated a Massachusetts statute that prohibited interception of wired communication. The U.S. District Court for Massachusetts, however, ruled that the two employees lacked any reasonable expectation of privacy. The District Court pointed out that reading e-mail after it had been transmitted did not constitute interception of wired communication. The court, moreover, cited several cases that negated a reasonable expectation of privacy for e-mail based on the use and transmission of e-mail information.[44] In 1999, for instance, an employee sued Microsoft for invading the privacy of his information and e-mail messages stored in personal folders on his computer. In this case, the Court of Appeals for the Fifth District of Texas decided that e-mail messages stored in "personal folders" but "were first transmitted over the network and were at some point accessible by a third party" lacked any reasonable expectation of privacy, even if those files were password protected by the employee.[45]

These legal precedents imply that there exists the potential for confidential data to be accessed by users who are authorized to monitor e-mail messages but not authorized to access confidential data, such as employee information. The implications of allowing unauthorized users to access confidential data have already become hot buttons of debate at Harvard. Although Harvard's Personnel Manual mentions that information should only be accessible by those who have authority to do so, the implied hierarchical chain of authority is left open-

[44] *Garrity v. John Hancock*, Civil Action no. 00-12143, 2002 U.S. Dist. LEXIS 8343, (D. Ma. May 7, 2002)
[45] *McLaren v. Microsoft*, 1999 Tex. App. LEXIS 4103, 1999 WL 339015

ended.[46] One question that may surface is whether those authorized to monitor employee e-mail are also authorized to view confidential information. If not, unnecessary desktop accumulation of such information may needlessly expose sensitive data to those who are not authorized to view or access confidential information. In these instances, the accidental peeping Tom may be trusted to ignore the confidential data or to notify his supervisors. The fact remains, however, that these actions would be taken after the opening of a potential Pandora's Box of confidential information, not before.

COMMERCIAL JOB DATABASE POLICIES: MONSTER, CAREERBUILDER.COM

The legal implications involved in privacy violations are also very important issues for many commercial job databases. Both Monster and Careerbuilder.com, two major commercial job databases, have already been victims of fraudulent attempts to access their pool of personal information.[47] The privacy statements of these websites are, therefore, very thorough and have adopted many of the guidelines put forth by the EU Directive. Monster, for instance, informs job applicants of how applicant information is used, distributed, and collected. Information is not distributed to third parties unless consent is given or the government makes a request. In addition, job applicants are told that their information is kept indefinitely, that they can at any time delete Internet-accessible information, and that they have the power to opt out of having their information placed in a searchable database.[48] Careerbuilder.com generally delivers the same privacy statement as Monster, but it does not inform job applicants of how long their information is stored. Careerbuilder.com, moreover, uniquely differentiates itself from Monster by specifically giving suggestions on how to identify email and online fraud pertaining to their website and by allowing job applicants to post information anonymously.[49]

---

[46] Lewis, *op. cit.*
[47] Kirby, Carrie. "Online Resumes Turn Risky." San Francisco Chronicle Times. 4 July 2005.
[48] "MonsterTRAK Privacy Statement." Online. 2003. Available: http://www.monstertrak.monster.com/intro/privacy.html
[49] "Protect Your Privacy and Safety." Careerbuilder.com. Online. 2005. Available: http://www.careerbuilder.com/JobSeeker/Info/Privacy.aspx

HEWLETT PACKARD PRIVACY POLICIES

Protecting privacy has also been large concern for U.S. companies that frequently traffic the information superhighway, especially those with global connections. Hewlett Packard, in particular, has taken a leading role in creating privacy policies that comprehensively protect the privacy of customer, employee, and job applicant information. In fact, in January 2001, HP became the first high-tech company in the United States to become certified by the U.S. Department of Commerce under the Safe Harbor framework.[50] The Safe Harbor framework was created between the U.S. Department of Commerce and the European Commission to facilitate U.S. business operations abroad without violating the EU Privacy Directive concerning data protection. Safe Harbor certification essentially ensures the EU that a certified company provides "adequate" privacy protection for personal data.[51]

The privacy policies in place at HP are extensive. The overarching HP policy is the Global Master Privacy Policy, which addresses the use and storage of customer and employee information. In addition to this policy is the Global Employee Data Privacy Policy which HP explicitly states addresses employee and job applicant information. Although the details of this policy are not publicly available, HP's general on-line privacy statement informs individuals of the use of their information, how they can change their information, and the security of their information. The seriousness HP takes to protect the privacy of its customers and employees, moreover, is substantiated by the existence of an HP Chief Privacy Office that handles the privacy issues of both customers and employees. The different mechanisms used by this office to ensure compliance with privacy policies are unique to HP in comparison to MIT and Harvard. All employees are required to have privacy training, and those handling confidential information must go through additional training. To increase awareness and compliance with these issues, Privacy Impact Assessments are used by employees in each project or sales and marketing program to make sure privacy policies are being upheld. Information Technology Application Development Questionnaires are used to evaluate whether or not privacy policies for Information Technology systems handling employee information are upheld. Moreover, HP operates an

[50] Statement of Barbara Lawler, Chief Privacy Officer of Hewlett Packard. United States. Cong. Senate. Commerce, Science, and Transportation Committee. Federal Privacy Legislation. 107th Cong., 2nd sess. Washington: GPA, 2002. Online. 8 December 2005. http://commerce.senate.gov/hearings/042502lawler.pdf

[51] "Safe Harbor." U.S. Department of Commerce. Online. 11 December 2005. http://www.export.gov/safeharbor/

internal privacy auditing system to review and to evaluate compliance with privacy policies.[52] Despite there being little indication of the effectiveness of such measures, these privacy protection mechanisms distinctly reflect a more proactive approach to protecting privacy by HP than by MIT or Harvard.

RECOMMENDATIONS FOR HANDLING OF JOB APPLICANT AND EMPLOYEE INFORMATION

In light of the privacy policies of Harvard, the European Union, the United States, commercial job databases, and Hewlett Packard, several steps can be taken to shore up the privacy holes that currently exist in the collecting and managing of job applicant and employee information at MIT.

Recommendations for Handling of Job Applicant Information

Job applicant information is unique in that no provisions for even protecting the privacy of this type of information exist at MIT, Harvard, or in federal or state law. The dangers associated with the leakage of this information, however, have already made headlines and should not deter MIT from preventing foreseeable information leakage. In policies specific to job applicant information collected through Webhire, MIT should post a privacy statement on the Staffing Services webpage that:

- Informs job applicants of the fate of their personal information and resumes
- Informs job applicants of the security measures taken to protect their information
- Allows job applicants to opt out of being put into a larger searchable database
- Allows job applicants to delete their personal information

In MIT Policies and Procedures, MIT should:

[52] "HP Approach." Hewlett Packard. 2005. Online. 8 December 2005. http://www.hp.com/hpinfo/globalcitizenship/gcreport/privacy/privapproach.html

- Include job applicant information under the definition of protected personal information in MIT Policy on Privacy of Information (Section 11.2)

Recommendations for Handling of Employee Information

Compared to job applicant information, employee information is explicitly mentioned in several MIT policies. These policies, however, should be updated to accommodate the implications of using modern computer-based technology in transferring and storing employee information. With regard to employee information handled through SAPweb, MIT should:

- Provide a privacy statement on SAPweb detailing how information is used and protected

With regard to employee information described in the HR Personnel Manual, MIT should incorporate new statements and changes that:

- Increase awareness among employees of the vulnerability of data sharing through electronic communication
- Increase awareness among employees of the vulnerability of data storage on desktops
- Clarify what is considered confidential information, including job applicant and employee information
- Require employees working with confidential information to either sign a confidentiality awareness statement or undergo privacy training
- Educate employees by providing examples and descriptions of how information can be accidentally leaked, e.g. viruses, DAT files, passwords, etc.
- Restrict the use of confidential information from being used unnecessarily

Recommendations for Handling of Both Job Applicant and Employee Information

Finally, for the handling of both job applicant and employee information, in MIT Policies and Procedures, MIT should proactively:

- Require using SSL enabled secure outbound SMTP authentication on all computers handling confidential information, including job applicant or employee information
- Require encryption of confidential information stored on computers in HR, IS&T, and all other departments to which confidential information is distributed and stored
- Require privacy training for employees and more in-depth privacy training for those working with confidential information, including job applicant and employee information

CONCLUSIONS

By implementing policy changes that primarily deal with redefining protected information, ensuring the security of the transmission and storage of protected information, and increasing the awareness of these issues, MIT will be in a better position to avoid information leakages that have been the nemesis of many other universities and information systems. Although this Institute may be perceived as a paragon of electronic infallibility, the construction of electronic information systems must give weight to the increased responsibility of protecting information channels that have or will soon be opened. Instead of taking a reactionary approach to the protection of job applicant and employee information, MIT should proactively step forward and avoid looming dangers by making small, incremental changes to the house that has been chosen to accommodate a continuously growing pool of job applicant and employee information.

APPENDIX

HARVARD JOB APPLICANT AND EMPLOYEE INFORMATION DATABASES

HIRES, the Job Applicant Tracking System

Compared to MIT, the resources in place to handle job applicant and employee information at Harvard are quite decentralized. Although an Office of Human Resources exists for the entire university, most of the human resources work is done in each of fourteen different human resources offices that exist for a particular department and/or employment sector.[53] In 1998, the Office of Human Resources was considering the adoption of an applicant tracking system that would connect many of these human resource offices and make collecting job applicant data more efficient.[54] By September 2003, Harvard followed through with this idea and began to only accept job applications and resumes through HIRES, a web-based applicant tracking system that handled the bulk of job applicant submissions.[55]

Based on the information available from the job application website, Harvard does not give job applicants the option of deleting their information or opting out of having their information placed in a larger searchable database. According to the website, "if you have not been contacted for the specific position to which you applied, for a period of time your resume also becomes available to recruiters seeking to fill other University positions.[56]" Although the website implies that job applicant information is available to recruiters for a period of time, no indication is given to job applicants of how long the information is stored in the HIRES system.

HARVie and PeopleSoft

The portal used to access databases housing employee information at Harvard is an intranet employee system known as HARVie. This system was launched in early 2004 and

---

[53] "Hiring @ Harvard." 2005. Online. 11 December 2005. http://www.employment.harvard.edu/careers/hiring/localhr.shtml

[54] "Highlights of EEO Practices at Harvard." *Harvard University Gazette*. 16 April 1998. Online. 6 December 2005. http://www.news.harvard.edu/gazette/1998/04.16/HighlightsofEEO.html

[55] "In Brief." *Harvard University Gazette*. 18 September 2003. Online. 6 December 2005. http://www.hno.harvard.edu/gazette/2003/09.18/06-notes.html

[56] "Hiring FAQs @ Harvard." 2005. Online. 6 December 2005. http://employment.harvard.edu/careers/hiring/faq.shtml

provides access to tools regarding employee benefits and services, the reporting of time and labor, general announcements, and the PeopleSoft Human Resources Management System (HRMS).[57] PeopleSoft is a web-integrated system that appears to be the Harvard equivalent of MIT's SAPweb system. PeopleSoft differs from SAPweb, however, in that the applicant tracking system HIRES feeds into the PeopleSoft system.[58,59] In order to access HARVie and other proprietary information, including Harvard employee policies, Harvard Personal Identification Number (PIN) authentication is required.

[57] "HARVie set to Launch on Feb. 18." *Harvard University Gazette*. 12 February 2004. Online. 6 December 2005. http://www.news.harvard.edu/gazette/2004/02.12/11-harvie.html
[58] "Welcome to the Online Help for ESS." A Better Learning Environment, Harvard University. Online. 2005. http://able.harvard.edu/hr-ess/
[59] "Welcome to the Online Help for Hiring and Personnel Actions." A Bette Learning Environment, Harvard University. Online. 2005. http://able.harvard.edu/hr-hiring/

ACKNOWLEDGEMENTS

This research would not have been possible without the help and encouragement of several people and departments to whom I would like to extend my warmest thanks:

Hal Abelson
Mike Fischer
Danny Weitzner
Keith Weinstein
Harry Lewis
MIT Human Resources
MIT Information Services and Technology