

The World Privacy Forum

2003 Job Search Privacy Study

*Job Searching in the Networked Environment: Consumer Privacy
Benchmarks*

November 11, 2003

Pam Dixon, Principal Investigator¹, Author

www.worldprivacyforum.org

| | |
|--|----|
| Index | |
| I. Executive Summary..... | 3 |
| II. Introduction | 8 |
| III. Principles of Fair Information Practices | 9 |
| IV. Core Job Site Privacy Issues..... | 11 |
| A. Collection of Job Seeker Data | |
| B. Use of SSN at Job Sites | |
| C. Use of EEO and ADA information Online | |
| D. Job Site Responses to Consumer Privacy Query | |
| E. Use of Third Party Cookies at Job and Career Sites | |
| F. NAI Principles: is Industry Self-Regulation Working at the Job Sites? | |
| G. Get vs. Post Requests on Job Sites | |
| H. Anonymous Access to Job Sites | |
| I. Trust and Seal Programs on the Job Sites | |
| J. Scope of Spam Issues Resulting from Online Job Searching | |
| K. Resume Sharing and Cross-Posting Issues | |
| L. Outright Resume Selling and Theft | |
| M. Frequency and Quality of Privacy Notices | |
| V. Privacy Issues at Specific Job Sites | 25 |
| A. USAJOBS.gov and StudentJobs.gov | |
| B. FastWeb.com | |
| C. Eliyon | |
| VI. Employment Application Kiosks and Sites | 28 |
| VII. Privacy Practices at Resume Writing Services | 35 |
| VIII. Privacy Practices at Resume Distribution Services..... | 42 |
| VIII. Best Practices at Career Sites | 50 |
| X. Consumer Guide to Online Job Sites | 52 |
| XI. Consumer Tips | 68 |
| XIII. Credits | 74 |
| XIV. Methodology | 74 |
| Appendix A: Key Unicru Screens | 81 |
| Updates..... | 82 |

I. Executive Summary

Job seekers, when applying for a job using electronic formats, experience less privacy and freedom than they do in non-electronic formats.

In a mere decade, job searching has evolved from primarily a paper and file-cabinet affair to an arena that is nearly completely digitized. Resumes, no matter what the originating form — fax, email, or paper — are now scanned, sorted, shuffled, stored and datamined in a bewildering assortment of ways. This changed applicant process has, overall, not had a beneficial effect on the job seeker.

Individuals looking for jobs have become part of a larger information superstructure which they may or may not be aware of. Tasks ranging from resume management to the electronic job application process have turned into data challenges and opportunities. If information equals money in the new economy, then resumes and their associated personally identifiable information have become the primary chattel of this digital job search, with job seeker activities on Web sites coming in at a close second.

Resume data, after all, is rich in information. Name, address, work history, educational information, and sometimes religious and even ethnic information may be gleaned from a job seeker's resume. Other types of information such as types of jobs looked at, salary range, willingness to relocate, and often much more is available from analyzing job seekers clicks and browsing patterns on job sites.

As the digitized pool of job seekers reached and then exceeded critical mass in the mid to late 1990s, entrepreneurs and others deeply understood how resume and job seeker data was valuable for more than simply job searching. Within the last ten years, and especially the last five, job searching has fundamentally changed, and it will not go back to what it was. The changes are deep, and they are structural.

In this new job searching structure, new ways of doing old things have emerged. Along with those, new uses for job seeker data have emerged. Among these new uses are legitimate, beneficial, and more efficient new ways of handling job seeker data. These uses, however, may in some cases extend well beyond job searching. Among the most egregious of these is identity theft, which is unfortunately now a well-documented issue in the job search arena.²

Less harmful but still problematic are the many marketing uses of job seeker data. In an information-rich, digital environment, the temptation to slice, dice, sort, store, and profile individuals is great, and companies engage in this practice far more than most people understand. Individuals who are concerned about giving out their credit card to engage in e-commerce may have the choice to resist a purchase. But a job seeker has little option to opt-out of an entire job search infrastructure that requires name, phone number, address, work history, educational history, and in some cases SSN and date of birth -- or no job opportunity.

Along with being newly digitized, the job search has become more commercialized. The numerous commercial companies dominating this digital job search space have so far not built a privacy-focused environment. Nor have they built a technology infrastructure that fully retains job seekers' abilities to look for employment without interfacing with sometimes multiple third party companies.

For example, it is nearly unthinkable for a job seeker to look for a job without visiting one of many large online job aggregating sites. While job seekers are focused on looking at jobs, at some sites, their every click is often noted for the record.

This report looks at the privacy issues involved in today's new job search processes. It documents what is happening to applicants right now, to their job search data and their resumes. It provides a snapshot of this significant part of the job search infrastructure.

The scope of this report focuses on what happens to job seekers from the point of creating a resume to the point of submitting it to a company. This report does not look at the large "back-end" hardware and software packages that operate inside hiring corporations to manage applicants. Resume writing services, online job search sites, employment kiosks, resume databases, Internet profiling databases, and resume distribution services are included in this study.

This study aims to document current privacy practices industry-wide, for better or worse. This study also seeks to benchmark state-of-the art consumer tips for job searching in the new medium.

A. Positive Findings

- Most job search sites are now posting privacy policies.
- Almost all job sites, when contacted with a consumer privacy query, responded to that query within two days or less.
- Fewer job sites require registration prior to looking at job ads. This represents a shift in practice from 2000/2001.
- More job sites, in contrast to studies conducted in 2000, are supporting anonymous access.
- There is a slight uptick in the job sites that allow companies to post full contact information in job ads. Full contact information in position announcements can in some cases allow job seekers to apply directly to companies. This reduces the number of third parties a consumer needs to interact with, which in turn reduces the risk of data spills.

B. Negative Findings

- Equal Employment Opportunity issues are particularly challenging to resolve in the online environment. The traditional standard of stating that disclosure of racial or ethnic information is voluntary and the information will be kept separate is not currently maintained consistently online. Further, some challenging new issues brought on by technology changes is emerging in the EEO area.
- Job seekers may look at job ads without registering at online job sites roughly 80 percent of the time, which is positive. However, the job ads do not always reveal enough contact information for the job seekers to actually apply to those jobs. Job seekers may apply to those job ads directly anywhere from one third to well over one half of the time. There is great variability in this depending on each job site and the ads offered at the time.
- Few job search sites display BBB Seals or TRUST-e seals.
- Many government and state-run job sites still request job seekers to submit their SSN and date of birth online prior to applying for jobs and in some cases, prior to looking at job opportunities.
- Consumers who post resumes on their personal home pages may be subject to apparent unethical spidering techniques by some companies. One company, for example, maintains a resume database of 250,00 resumes it has indexed and spidered.³
- Job seekers are routinely asked to give up a great deal of personal information online. There is an overall pattern of job sites not limiting their information collection as tightly as is possible.
- The use of third party, persistent cookies has increased on job sites. The self-regulatory NAI Principles the advertisers who deposit third party cookies voluntarily subscribe to are not being adhered to well. Research found that cookies were in some cases present on pages where resumes were input.
- Along those lines, research found that the information job seekers entered into forms was frequently placed in “URL strings” on pages with third party cookies, thus passing off the job seeker information to advertisers and other third parties with banner ads and other technologies on the pages.
- Job search sites have become much more sophisticated about finding legal ways of sharing job seeker data. Job seekers may not know when data sharing is occurring because it has become less obvious.
- Privacy policies industry-wide are generally not highly compliant with all eight

principles of Fair Information Practices.

C. Key Consumer Findings

- Job seekers need to completely retool the way they approach the job search. Implementing new, updated tips for a commercialized, digitized job search is key for job seekers who care about their information privacy.
- Job seekers need to pay more attention to the types of cookies they are storing in their computers. While cookies are a simple technology, consumers need to know that in the current job search, certain kinds of cookies can be very privacy-invasive.
- There are new methods of finding a more or less direct pathway to corporations. This report outlines those findings for consumers.
- Instead of evaluating job search sites by size or brand, job seekers need to learn new ways of evaluating job search sites by privacy markers. These markers are explained and listed in the consumer section of this report.
- Job seekers need to educate themselves on key privacy and background check issues at employment application kiosks, as these kiosks represent a significant national employment trend.

D. Specific Privacy Issues

- Unicru, a company that processes an estimated one applicant per second, has installed 14 thousand-plus employment kiosks throughout the United States at major retailers and elsewhere. The kiosk employment applications researchers tested request that job seekers supply their SSN, date of birth, and agree to an instant background check – all without a posted privacy policy at the kiosks. The kiosks that researchers tested revealed additional issues relating to meaningful withdrawal of electronic consent.
- FastWeb.com, a popular online college scholarship search service and the largest ranked educational site on the Web, is owned by Monster.com. FastWeb in its online student questionnaire asks for detailed personal information. For example, students may choose to answer questions about sexual orientation, medical illnesses, and other highly sensitive issues. What specifically is done with this sensitive data? According to the FastWeb privacy policy, the company can share this data if a student opts in.
- Researchers have submitted a Freedom of Information Act request regarding USAJOBS.gov and StudentJobs.gov. These two sites are the Federal

Government's official job sites. In the privacy policy posted at these sites, no mention is made that Monster.com is the government contractor that is operating these sites.

- Eliyon, a technology company based in Cambridge, Massachusetts, has built a database of more than 16 million executives in approximately 1,055,935 companies.⁴ This database is accessible to and searchable by anyone with a Web connection. The database contains detailed profiles on individuals based on information the company gathers from the Internet, among other sources. It sells these profiles to marketing companies and to recruiters. Researchers found that the database contained many errors and revealed personal information, for example, childrens' names in one case. The database does not have a privacy policy posted and does not yet have an opt-out arrangement for those profiled.
- As previously reported in a preliminary study February, 2003, HotResumes.com outright sold more than 4,900 job seeker resumes that had been entrusted to them. The resumes were sold to another job site apparently without job seeker permission. Although the matter is now resolved, a person posing as a recruiter gained access to resume databases and stole resumes from those databases for his own personal use.

E. Recommendations

- We urge the FTC to look at the amount and kind of job seeker data that is routinely gathered at job sites and to investigate how it is actually being used in some cases. We also urge the FTC to look at any potential FCRA issues arising from the increasingly widely-deployed employment application kiosks of varying types.
- We urge the EEOC to carefully consider how Title VII guidelines are being satisfied in the new online application processes. We also urge the EEOC to carefully consider and investigate the new crop of "diversity targeting" technologies and techniques for their legality and fairness under Title VII.
- We request that SHRM, NACE, and other non-profit employment industry associations work with a coalition of privacy groups, consumer advocacy groups, and national labor organizations to outline complete guidelines that codify online application privacy protocols for the purpose of protection of job seekers.
- We request that Congress investigate the practices of the online job search industry and help shape, define, and encourage a discussion of potential consumer protections and standards.

II. Introduction

This research was conducted with several purposes in mind. First, it set out to document and benchmark the privacy practices at the leading job search sites and list those practices openly so consumers could make informed decisions about each site based on fact.

The second goal of the study was to take a snapshot of the overall privacy practices of the job search industry, and using the core principles of Fair Information Practices as a guide, document those practices.

A third goal of the study was to assess what kinds of personal information job search sites were generally collecting from consumers, and how the sites were using that information.

And finally, the fourth goal of the study was to assess the question: is job applicant privacy enhanced or diminished in the online environment?

The report has set out a consumer listing of 53 job search sites that were tested extensively in order to meet the first goal of the study. The consumer listing gives detailed factual information about how each job site is operating relevant to privacy concerns. Listing of a privacy policy, registration requirements, and presence of persistent third party cookies are examples of the items detailed. A detailed set of consumer tips for online job searching is included in the study to help consumers make informed choices as they look for work online.

With the core Fair Information Practices in mind, the study conducted wide-ranging research on the job sites to acquire information about their practices and privacy statements. To assess the kinds of information the sites were collecting, researchers posted test resumes at each site and applied for jobs online. The results were collected and analyzed to get an applicant's viewpoint of the way the resume information was handled. Other areas of the applicant process were also reviewed, assessed, and analyzed.

After the research results were finalized and analyzed, core privacy issues were observed and documented from the results. The study sets forth this core discussion of job applicant issues, best practices, and areas of concern that address the second and third study goals.

And finally, the study makes recommendations to industry groups, Congress, the EEOC and the FTC based on the researchers' assessment of the answer to the fourth goal of the study.

Is job seeker privacy enhanced or diminished in the online environment? This report finds that it is substantially diminished. However, some bright spots exist. This report strives to fairly document as full of a spectrum of these issues as possible.

III. Principles of Fair Information Practices

The premise of this report and the analysis of site practices and issues in this report is based upon the canon of Fair Information Practices, particularly as expressed in the eight principles of Fair Information Practices outlined in the **Organization for Economic Cooperation and Development (OECD) 1980 Guidelines**.⁵ These guidelines form the basis of most modern international privacy agreements and national laws. The principles were agreed upon by member countries, including the United States. These principles and guidelines are referred to throughout the report either as the principles of Fair Information Practices, or as the OECD guidelines.

A. The OECD Guidelines outlining the principles of Fair Information Practices are as follows:

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above. The United States endorsed the OECD Guidelines.

B. Other Documents Considered

An historic set of fair information practices was created in July 1973 by the United States Department of Health, Education and Welfare's seminal 1973 report entitled *Records, Computers and the Rights of Citizens* (1973). Typically referred to as the "HEW Report," its core principles are as follows.

The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.⁶

For more information about these principles, please see U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, computers, and the Rights of Citizens* viii (1973).

The European Union Directive on the Protection of Personal Data (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996) are other major documents that reinforce the OECD core principles. While these documents were considered in the preparation of this report, they did not form the immediate backbone of the study and the report.

IV. Core Job Site Privacy Issues

The following issues are highly relevant to job applicant privacy as found in the research conducted for this study.

A. Collection of Job Seeker Data at Job Sites

Job and employment sites consistently collect robust, rich information from job seekers. Most sites collect the following kinds of information from job seekers:

- name
- address
- phone number
- salary
- educational level
- future educational plans
- geographic location
- years on the job
- willingness to travel or relocate.

Some sites may request gender or race to comply with EEO regulations. Some sites may request a date of birth as well. Only a handful of sites in the study collected SSNs. However, those sites had significant reach. For example, USAJOBS, the US Government's Web site, requests SSN when job seekers want to post a resume.

All or part of the aforementioned data, plus the information contained in the resume is what job sites typically collect from job seekers looking for jobs.

In recent years, some job sites have begun selling services such as resume distribution to job seekers. When this is the case, then these sites also may collect credit card data.

Some employers may also gather personality profiles from job seekers via an online application form. Sports Authority is an example of an employer that collects this type of data.

Even when a job seeker simply browses through a job site looking at job ads without registering or posting a resume, the sites may still collect certain pieces of data from job seekers such as types of jobs searched for, where, and so on. This type of collection is usually accomplished through a combination of depositing cookies and using page referrals, and may be stopped by consumers who are aware of the activity.

Some "pass through" sites, such as DirectEmployers.com, stand as an exception to the large quantities of personal data collected at employment sites in that these sites gather

almost zero job seeker data; the goal there is to send job seekers to the corporate Web site where the job is located. Another pass-through site is Jobs.com. Jobs.com, though, is slightly different in that it takes job seekers to job ads posted on a third party commercial Web site.

Few online businesses provide as rich and steady of a supply of detailed consumer data as job sites do. The “pass through” sites prove that most sites could be gathering much less information from job seekers.

B. Use of SSN at Job Sites

In this study, the sites that requested Social Security Numbers included government, state, and teacher (state –run) sites. Commercial sites related to Unicru also requested job seeker SSN and date of birth. While only a handful of sites requested this information, the sites that did request it had a very broad reach.

Specifically, USAJOBS.opm.gov and StudentJobs.gov allowed applicants to browse job ads without divulging an SSN.⁷ However, to post a resume on the sites, research found that job seekers had to disclose SSN. According to an OPM press release, just from August 4 to 20th of 2003, job seekers created more than 51,000 resumes on the site,⁸ which gives a fair idea of the impact of the SSN request at the USAJOBS site.

EdJoin (a site for California Teachers) allowed voluntary disclosure of SSN. CalJobs (www.caljobs.ca.gov), the site for California State jobs, requested disclosure of job seeker SSN and date of birth prior to looking at a job ad.

Sports Authority stores, which request job applicant SSN and date of birth prior to accepting even a job application, like the other sites, did so electronically.⁹ However, these stores have the distinction of being the only known sites in this study to request an SSN and date of birth from job applicants without also posting a privacy policy governing the use of that data.

Sports Authority is operating Unicru-run employment application kiosks and a matching Web site. Unicru processes approximately one applicant per second, or an estimated 6 million applicants per year who must go through that process.

So, just in this study, the sites that require SSN for application impact well over 6 million people per year.

Given that identity theft has been identified by experts as an “insider job,”¹⁰ it is important for job sites to shift away from the use of SSN as an identifier. In the case of Unicru, which is conducting instant background checks on applicants prior to allowing an applicant to submit an application, it will be important to at the very least encourage this business to adopt the practice of posting a privacy policy at the kiosk and its related Web sites that outlines how the SSN and other information will be stored and handled.

C. Use of EEO and ADA Information Online

Research has found that online job sites have been highly inconsistent with how Equal Employment Opportunity (EEO) information is applied. Overall, sites tend to be more careful and consistent with Americans with Disabilities Act (ADA) issues.

Title VII of the Civil Rights Act of 1964 prohibits employment discrimination based on **race, color, religion, sex, or national origin**.¹¹ The rules for applying the provisions of Title VII requires employers or employment agencies to state that any information related to EEO questions is completely voluntary. The employer must also state that the information will not be included in a jobseeker's application to the employer.

By far the site with the clearest compliance with these provisions is Unicru's as seen at Sports Authority. This is what its EEO notice looked like at SportsAuthority.com:

The following questions are completely voluntary. To comply with government regulations we must make a good faith effort to record this information on our applicants. Your answers will not be made available to anyone involved in the hiring process.

What is your race?

American Indian or Alaska Native

Asian

Black or African American

Hispanic or Latino

Native Hawaiian/ Other Pacific Islander

Caucasian or White

Sex:

Male

Female

Thank you.

This is a faultless application of EEO guidelines in an online application environment. But few sites go this far. For example, when Job.com asks for gender and date of birth, there is not an EEO notice stating that giving the gender information is voluntary. This kind of request is actually not uncommon at online job sites.

FastWeb.com raises more complex EEO questions. FastWeb is a college scholarship search site. The site, which is owned by Monster.com, asks for students' gender. It also allows students to respond to questions about nationality, religion, and some medical disabilities. These are EEO questions. But the site, being a scholarship search site, does not fall under the category of being an employer or employment agency, which is what would make the Title VII regulations apply. However, the FastWeb privacy policy notes that if a student opts in, then their information may be shared with a potential employer.

In the course of research, researchers became aware of a document that discussed Monster.com's use of the FastWeb site for hiring part-time workers. This potentially places FastWeb in the category of an employment agency, which would require the site to give EEO notice regarding the voluntary submission of racial, gender, religious, and nationality information. It would also, according to the current rules, require that FastWeb keep the Title VII data separate from a user's application.

The EEO guidelines are being stretched by new technologies and the new online application environment. The EEO regulations either need to be updated for electronic mediums, or the old guidelines need to be reaffirmed and applied in the new mediums.

D. Job Site Responses to Consumer Privacy Queries

As part of the Job Search Privacy Study, researchers conducted a test of email responses to privacy questions. The test was conducted via email without the foreknowledge of the sites. Wherever possible, researchers emailed a query to the email address listed on the site privacy policy.

The goals of the privacy query test were to determine:

- How sites responded to consumer privacy queries
- The accuracy of the contact information listed on the privacy policy
- If a site did not post a privacy policy, the goal was also to determine if the site would give appropriate privacy assurances to consumers.

Researchers compiled a list of the email addresses from the privacy policies at the job sites in the study. For sites that did not post a privacy policy, the email address was taken from the site contact information available at the site or from the most obvious point of contact, for example, an email address listed on the home page or customer support or feedback page.

A very basic email¹² was crafted to test the privacy-related help a consumer might receive at the job search sites. A question about SSNs was added for sites that collected that information. For sites that possibly marketed information to advertisers, slight variations in the email were made to accommodate this aspect. The email was sent using an email address that was not easily identifiable as belonging to either a privacy organization or privacy researchers.

The queries went out September 16, 2003. The first responses began to arrive within approximately one hour. The last response researchers received arrived September 30, 2003. The test officially concluded October 15, 2003. Researchers sent repeat queries to unresponsive sites up until November 7, 2003.

There was some attrition in this study due to spam filtering, mail bouncebacks, and other unavoidable technical glitches. Even taking that into account, it is clear that the job sites took the consumer query seriously. Most sites replied to researchers in under two days, which is quite rapid by most standards.

1. Specific Site Responses

a. The following job sites sent personal emails back to researchers' privacy queries in under 6 hours.

- CareerBuilder
- WorkingWorld
- Net-Temps
- MonsterTrak
- NationJob.
- Workopolis.com
- Medzilla.com
- Resume.com
- EdJoin.org
- LegalStaff
- DirectEmployers
- WetFeet
- NACELink
- EDD/CalJobs
- IM Diversity

b. The following sites sent an auto-reply response in under 6 hours:

- FlipDog
- *TrueCareers – site followed up with additional reply later.
- Monster.com
- Teachers.net
- Craigslist.org
- **CareerBuilder The autoresponse CareerBuilder sent within 6 hours came after it had already sent a personal response to researchers' privacy query email. The autoresponse from CareerBuilder requested that the researcher fill out a followup customer satisfaction survey.
- CollegeCentral.com
- *FedJobs.gov (USAJOBS) – site followed up with additional reply later.
- *CollegeRecruiter – site followed up with additional reply later.

c. The following sites sent a response within 6 to 24 hours:

- OPM.gov
- FedJobs.gov USAJOBS
- ExecuNet
- CollegeRecruiter
- IHire.Inc.
- FastWeb
- DICE.com
- TrueCareers – Sent a detailed SallieMae privacy policy explanation.

d. The following sites sent a response in over 48 hours:

- FedJobs – Federal Research Service.
- OPM –
- HireDiversity.
- WorkStream Inc. (6 Figure Jobs

2. Unresponsive Sites / Technical Issues

Researchers conducted the privacy email query test for several purposes. One was to see the responses. But the test was also conducted to see if the email addresses companies listed on privacy policies were accurate. Before the test was conducted, researchers included in the methodology the fact that new site addresses were not to be searched out and tried, which would create a lack of fairness for those sites that had listed accurate addresses in their privacy policies.

a. The following are sites, when after being emailed and retested, did not bounce back replies to researchers:

- Saludos.com –Email was sent to info@Saludos.com.
- CareerJournal - Email was sent to the address list on the CareerJournal privacy policy, <cwc-news@interactive.wsj.com>
- Vault – Email was sent to feedback@staff.vault.com
- Careersite – Email was sent to empwiz-support@careersite.com
- Ocjobs – Email was sent to info@ocjobsite.com
- Careereplorer - Email was sent to info@careereplorer.net

b. Very few total addresses in this study came back as undeliverable to researchers. Those that did are included in the list below.

- info@job.com
- webmaster@brassring.com
- rci@bestjobsusa.com
- info@jobbankusa
- Andrew.lin@adecco.com **
- russ@idealist.org***

* Researchers retested and checked all of these messages for accuracy. Email addresses were tested more than one time after a bounce.

** After researchers completed the email test, Adecco completed a major Adecco USA site redesign that addressed the response problems.

*** Idealist's email system was down during the test period.

E. Use of Third Party Cookies at Job and Career Sites

The use of third party cookies¹³ has grown at career and job-related sites.

For background, cookies are bits of information that can be sent to a computer. A Web site an individual is visiting can send a cookie, and so can a company that has a banner advertisement on a page of the site. For example, if an individual is visiting the Web site www.abc.com, a cookie from www.12345678.com would be considered a third party cookie. Third party cookies come from sites other than those an individual has directly navigated to.

Third party cookies may expire anywhere from one day to several decades. Cookies that take more than 6 months to expire are called long term tracking cookies, or persistent cookies. Many of the companies that use persistent cookies are national advertising companies. These companies, because they are using cookies across many sites, are able to develop broad consumer profiles based on Web behaviors if the tracking cookies are accepted and left on.¹⁴

Most large job search sites have relationships with one or more national advertising networks, including DoubleClick, Advertising.com, Omniture, or others. Privacy notices at these sites often provide mundane descriptions of cookie use, frequently explaining that cookies serve to make using the site more efficient.¹⁵

Research disclosed that third party cookies are being used in the resume upload areas of career sites.¹⁶ This provides information to the advertisers that the consumer has likely uploaded a resume and is likely actively looking for a job. Financial advertisers desiring to sell loans may be very interested in finding the people who are out of work.¹⁷

Many believe that since cookies generally only collect computer IP addresses, that cookie data is anonymous.

That is actually not always true. If a user at any point has accepted a third party long term tracking cookie and then has filled in a survey, a Web form (including online job forms at third party career sites) or has purchased something online at a site using the advertiser that set the cookie, depending on the privacy practices of that site, the users IP address may have been correlated or “matched” to the person’s name, home address, and other information the user filled in.

A recent issue complicating the collection and storage of user IP addresses in persistent cookies by national advertisers are the new legal uses for that IP address. The RIAA v. Verizon lawsuit¹⁸ paved the way for copyright owners to subpoena personal records connected to specific IP addresses by showing only the most minimal justification. If a marketing company has collected users IP addresses, it may now express that it has a copyright concern, and legitimately subpoena the user information attached to that IP address. If a user has not already supplied personal information to an advertiser, it is still no longer that difficult to acquire.

The practice of setting persistent cookies on resume pages should ideally be discontinued. And all job sites allowing cookies from member companies of the NAI Principles need to familiarize themselves with those agreements and provide direct links to the NAI opt-out notice.

Meanwhile, consumers should know that some types of cookies are not the innocent residents of hard drives that job sites insist them to be.

F. NAI Principles: Is Industry Self-Regulation Working at the Job Sites?

The NAI Principles were forged between the FTC and a group of national advertisers in 2001. The idea was for the advertisers to self-regulate their online consumer profiling activities, and thus forestall legislation. As part of that self-regulations, the advertising networks designed an “opt-out” cookie, which if a user downloaded, would stop the consumer from being tracked by the company. Advertisers were to provide links to the opt-out cookies in privacy policies on affected Web sites.

Currently, almost no career-related site using third party cookies of NAI members¹⁹ actually links to the appropriate opt-out pages. It appears that self-regulation is not working well, at least not at the online job search sites.

Of the 13 companies in the study that needed to provide one or more opt-out links, only two fully did so.

1. Provided opt-out link:

- CareerBuilder: provided Omniture opt-out link.
- Vault: provided NAI opt-out link.

2. Did not provide opt-out link:

- 6FigureJobs: ValueClick, no opt out link.
- CaliforniaJobs.com: Fastclick, no opt-out link.
- CareerJournal: Link to DoubleClick privacy policy instead of required opt-out page.
- CareerSite: Omniture, no opt out link.
- CollegeRecruiter: Doubleclick, no opt out link.
- College Grad Job Hunter: Doubleclick, Advertising.com. Opt out is available for Doubleclick, but not for Advertising.com.
- DICE: Doubleclick, no opt-out link
- HireDiversity: Doubleclick, Bluestreak; neither linked to opt-out.
- Job.com: advertising.com, no opt-out
- Monster.com: Doubleclick, atdmt, BlueStreak; no opt-out links.
- MonsterDiversity: Bluestreak; no opt-out link.

G. Get Versus Post Requests on Job Search Sites

Web browsers do one thing very well: they provide a friendly graphic interface for individuals to use as they search Web sites. But behind the pretty graphics, browser commands coded into Web pages may be used to put job seeker information entered into Web forms into a browser's URL bar. Once that information is in the URL bar, the information can then be picked up by advertisers that have a presence on that same page.

This "picking up" of job search data generally grabs job search keywords, salary, location, willingness to relocate, and the specific jobs a person looks at, and when. Any words or items job seekers fill into a Web form can be captured.

This kind of information spill is occurring very frequently on job search sites. It may strike some as "small potatoes" in terms of data. But these not-insignificant data pieces may be combined with other bits of data across many Web sites, particularly by national ad networks. The final result of this kind of profiling may be an unnervingly accurate portrait of the computer user in question.

1. How it works

Web sites may gather information from Web forms two fundamental ways. The site may

get the information by using something called a POST request, which simply grabs the information from a Web form and sends it to the Web site a user is visiting.

Or the site may get the information using a GET request. A GET request in the HTML code takes the information that has been entered into Web forms and places it in the URL, or Web address, of the following page. This is where a job seeker who has entered job search information can get into trouble.

While it sounds very simple, it is actually a negative privacy practice to put job search keywords or data into the URL bar. Any information placed in the URL may be freely picked up by advertisers with banner ads on that same page.

For example, CollegeGradJobHunter has a page on which job seekers may click on specific jobs that interest them. At the time of research, the page contained banners served by Advertising.com, a national advertising company that deposits long-term cookies that may track consumers over many years as they browse the Web.

A banner ad is able to pick up any GET requests, and any information that shows in the URL string, or box on the top of the browser window. On the CollegeGradJobHunter page, Advertising.com was delivered a “referrer string” or a line of code that gave it information that a person with a specific computer address was looking at an accounting job.

This is what the URL string, or URL showing in the browser window, looked like:

```
http://jobs.collegegrad.com/jobdetail.cfm?job=1757120&keywords=accounting%20
```

It worth mentioning again that if a person has filled in a Web form, a survey, or has in some other way provided their name and email to a site with Advertising.com cookies, then Advertising.com may be able to correlate the “anonymous” data about searching for an accounting job with a name, address, or email address.

This use of GET requests is fairly common. Researchers found GET requests at sites from large to small. At Job.com, researchers searched for a job using the keyword **Accounting**. Researchers found that Job.com used a GET request to throw the information up into the URL box, or string.

The GET request looked like this:

```
<form action="/jobsearch/index.cfm" method="get">
```

The code above is directing the information in the Web form to be placed in the browsers URL box. The address that showed up in the URL box in the browser after doing the keyword search looked like this:

```
http://www.job.com/jobsearch/index.cfm?tid=search.cfm&stype=1&ca tbox=0&stbox=5&key1=accounting+
```

Note that at the end of the URL, the keyword accounting shows up clearly. And on the very next page, an ad banner from jobclicks.net took up the information in an i frame, and off it went to jobclicks.net to add a little bit of data to an ever expanding profile of an accountant searching for jobs online.

```
<ifr'+ame
src="http://ads.jobclicks.net/ads/banman.asp?ZoneID=30&Task=Get&SiteID=2&X
=' + browDateTime + '&keywords=G5,I0,accounting," width=468 height=60
Marginwidth=0 Marginheight=0 Hspace=0 Vspace=0 Frameborder=0
Scrolling=No></ifr'+ame>');
// -->
```

Finally, after posting a resume on the Job.com site, the following URL was placed in the URL box with a GET request:

```
http://www.job.com/jobsearch/index.cfm?tid=applyOnline.cfm&s=2&i=272542&o
=29&catBox=0&StBox=5&SalBox=0&key1=accounting&pCity=&pTitle=&sType=1&jc=0
&lst=0&jobchan=&stUsing=0&ns=0&stFresh=60&resPg=20&vMode=x&sCol=1&sDir=1
```

The URL address, which could be retrieved by a banner ad, clearly shows that someone had applied online for a job, what kind of job they applied for, and what city the job was in. If there are no third parties on the same page as this URL string, then all is well. But if there are any third parties at all, then there is a data spill.

The spilling of job seeker information through GET requests is unnecessary. Job sites may display ads without giving the advertising networks sensitive job seeker information that can be used to create a consumer profile of that job seeker. Switching to POST requests would go far in enabling consumers to search for jobs without spilling keywords and other information about their job search interests.

H. Anonymous Access to Job Sites

Researchers tested each job site in the study to see if it allowed anonymous access, and if so, researchers tested how much a job seeker could accomplish anonymously. Except for some javascripting issues,²⁰ most sites do allow anonymous access.

There are no known sites intentionally blocking anonymizing services. Those sites that did not allow true anonymizing services, still allowed the use of proxies.²¹

If a job site posted ads containing complete employer contact information, and especially an email link to an employer's email address, researchers were able to look for jobs anonymously and then apply online anonymously. Given the third party tracking occurring at some of the job sites, this is an excellent option for job seekers to take.

For a comprehensive list of anonymizing sites and services, please see the EPIC page which maintains a good list. <<http://www.epic.org/privacy/tools.html>> . Scroll down to "Surf Anonymously."

I. Trust and Seal Programs on the Job Sites

Seal programs have a particular importance in the online job search arena. Job seekers using Web sites to look for jobs are asked to give up detailed, personally identifiable information to these businesses. More and more, job seekers are also paying for extra services such as “resume upgrades” at these same sites, increasing the privacy and security risks by adding financial data into their data mix.

Seal programs such as those offered by TRUST-e and the BBB’s Online division are part of the solution for consumers. These programs can help job seekers make informed business and privacy decisions prior to releasing personal information. Of particular help is the BBB program which has a long-standing, well-oiled complaint reporting system already established from its physical BBB bureaus located throughout the United States. Consumers may look at the past numbers and types of consumer complaints and have an effective, unbiased means to gauge a business’ approach to consumers.

Researchers found that a very small percentage of sites were members of any seal program. Those members of the job and career industry that have joined seal programs and are in good standing deserve credit and praise, especially given the strikingly low overall membership among this sector.

It should be noted that some job sites display seals fraudulently. Despite their best efforts, the seal programs have had difficulties with sites that “spoof” or fake the seals. Both the BBB and TRUST-e warn that sites that display spoofed seals may be fraudulent.

As a note, both organizations use "click-to-verify" seals that, when clicked on, take consumers from the Web site displaying the seal directly to an official, verified page on the seal granting organization’s site. For the BBB seals, the seal is dated, and links to customer service reports about the business. TRUST-e uses a list of licensees for verification.

Sites spoofing seals will often take out the link to the seal verification site, so the seal no longer clicks through. Some seal-spoofing sites actually link to the seal organization’s home page to imply that the seal is valid. This is a deceptive practice.

The link to a good BBB seal, for example will look like this:

<http://www.bbbonline.org/cks.asp?id=102121314211724370> .

Note that the URL contains an id number.

If a site fraudulently displays a BBB seal, the BBB will still hold the offending site to the standards of the seal. Consumers may enter arbitration even in absence of the company displaying the seal inappropriately.

1. Job Site BBB Seal Members in good standing:

- IHire
- ResumeDirector
- ResumeXposure
- ResumeRabbit

2. Job Sites Displaying a BBB Seal in Violation of a Seal Program:

- MonsterTrak.com (Expired Privacy Seal, deceptively linked .)
- ResumeBlaster Expired Reliability Seal.)
- Resume.com (Expired Reliability Seal, link deactivated.)
- JobViper (Expired Reliability Seal, deceptively linked.)
- ResumeBroadcaster.com (Up to date seal, but technical violation of Reliability Seal terms: no posted privacy policy.)

3. TRUST-e members in Good Standing:

- WetFeet
- HotJobs
- Unicru

J. Scope of SPAM Issues Resulting from Online Job Searching

The dimensions of spam problems resulting from posting a resume online has changed significantly at job sites in the past three years. In the past, just about any resume posted online would attract a good deal of unsolicited email.

However, the larger sites in general and highly security conscious niche sites have cracked down hard on this problem. Monster.com, HotJobs, Medzilla, Craigslist.org, and LegalStaff are among those sites that did not spread a single piece of unsolicited email after a resume was posted on the site. Generally, Internet business models have become much more sophisticated and do not rely on sending advertising emails to make a profit.

That being said, some sites still do have a problem with spam. Much of the spam took the form of “affiliate marketing,” a practice where people send out links suggesting jobseekers visit certain sites. If the jobseeker visits the site, the individual sending the email will make some money from the referral. Some affiliate marketing messages were deceptive, and were made to look as if they were coming from a recruiter.

This problem is especially pervasive among some resume distribution services.

K. Resume Sharing and Cross-Posting Issues

Undisclosed resume sharing among the job sites is not as widespread as it once was. However, the practice has not completely disappeared. Researchers experienced this issue at three sites. SanDiegoJobs.com, CollegeGradJobHunter, and JobWareHouse.

After researchers posted two separate test resumes at SanDiegoJobs.com, both of the resumes were then discovered on JobWareHouse.com. JobWareHouse in fact sent email messages stating that the resumes had been received from San Diego Jobs, and the site was posting the resume for the researchers and providing a logon name and password. JobWareHouse sent one additional email to researchers test resumes from CollegeGradJobHunter stating it had received the resume from an affiliate.

The SanDiegoJobs.com site does not disclose the resume cross-posting to job seekers in its privacy policy.²² SanDiegoJobs.com is part of a larger network of sites such as Orangecountryjobs.com, etc.

The email trail below shows what happened to the resume posted on CollegeGrad Job Hunter, LanceE7. This test resume was posted August 12, 2003. It received very little email. On October 2, JobWareHouse.com notified the LanceE7 resume that it had received the resume from an affiliate and had set up a user ID and password.

After that time, because of the commingling of the two sites, it became nearly impossible to tell which email came from which site. To give an idea of the resume response pattern, here are the exact results from the first resume posted at CollegeGradJobHunter.com:

| | | |
|--------|--|---|
| Date: | Email From: | Topic: |
| 030827 | jfirth@spectranet.ca | use BlastMyResume |
| 030831 | seekwork.net | visit site |
| 030915 | plugincareercenter.com | visit site |
| 030929 | execs-direct | post here |
| 031002 | jobwarehouse.com | received resume from affiliate - set up uid and pw |
| 031002 | jobwarehouse.com | welcome |
| 031002 | jobwarehouse.com | newsletter/ |
| 031002 | jobwarehouse.com | newsletter |
| 031002 | jobwarehouse.com | newsletter/ |
| 031002 | jobwarehouse.com | newsletter |
| 031004 | jobwarehouse.com | newsletter/ |
| 031005 | jobwarehouse.com | newsletter/ |
| 031006 | jobwarehouse.com | newsletter/ |
| 031006 | jobwarehouse.com | newsletter/ |
| 031005 | execs-direct | use ResumeRabbit |
| 031007 | resumes2work.com | submit resume |
| 031007 | jobwarehouse.com | newsletter/ |
| 031007 | jobwatchers.com | post here |
| 031008 | jobwarehouse.com | newsletter/ |
| 031008 | jobwarehouse.com | newsletter/ |
| 031008 | ammassociates | use our services |
| 031009 | jobwarehouse.com | newsletter/ |
| 031009 | job2@ijonn.com | click to go to www.eorss.com |
| 031010 | jobwarehouse.com | newsletter/ |
| 031010 | familyprima.com | financial planning |
| 031011 | jobwarehouse.com | newsletter |
| 031012 | execs-direct | use resumemailman |
| 031013 | jobwatchers.com | post here |
| 031013 | jobguru.com | post here |
| 031013 | jobwarehouse.com | newsletter |
| 031014 | careerXpress.org | visit |
| 031020 | execs-direct | use ResumeRabbit |
| 031021 | yahoo.com | click to go to employment job center |
| 031023 | execs-direct | use "yourjobsearcher" |
| 031023 | jfirth@outer-net.com | use ResumeRabbit |

Researchers found the cross-posting confusing, even with highly unique resume addresses. Cross-posting resumes should only be done with prior explicit consent from the job seeker. In this sort of situation, a double opt-in is appropriate in order to provide adequate assurances that job seekers have been well-informed of the cross-posting and have in fact agreed to it prior to the time it happens.

It is critical for consumers to keep excellent track of their resumes so they know when this kind of thing has happened to them.

L. Outright Resume Selling and Theft

Researchers found one instance of known, provable resume selling and two instances of known, provable resume theft.

In November 2002, HotResumes.com sold 4,941 resumes for .33 cents each to a now-defunct job site called BioTechCareers.com. This invoice was made public and was published as part of a lawsuit against an individual who had purloined resumes from other resume databases, a Mr. Monastra. (*Medzilla vs. Optimum Intelligence et al.*)

²³The invoice was noted as a "resume sale" and it was marked as paid. ²⁴

For reference purposes, the HotResumes privacy policy that was posted on its Web site at the time is quoted below in part.

HotResumes.com privacy policy excerpt from February, 2003:

"We do not disclose information about your individual visits to HotResumes.com, or personal information that you provide, such as your name, address, email address, telephone number, credit card number, etc., to any outside parties, except when we believe the law requires it. But, we may record and share aggregated information with our partners."

HotResumes has since changed its privacy policy. It is unknown if the site is still selling resumes or not.

Beyond the theft of resumes in Medzilla's and other databases by Optimum Intelligence, one known offline resume heist has occurred. In October, 2003, a company, ELS Locators requested a copy of the file of all New Jersey residents who had applied for unemployment benefits. The company then set up a three-day job fair through New Jersey's State Department of Labor office. The job applicants attending the fairs gave ELS Locators a \$42 fee plus their Social Security Numbers, bank account numbers and credit card information.

In November, Federal authorities contacted New Jersey law enforcement officials and told them that ELS was a fraudulent company that had perpetuated identity theft scams in 15 cities in eight states. ²⁵

It is critical for job seekers to understand when SSNs should and should not be given prior to an interview. Some legitimate employers (such as Sports Authority and other businesses using Unicru employment application kiosks) require applicants to give up a Social Security Number and date of birth before even filling out an application, but overall, this is rare. However, no employer needs bank account information or credit card numbers upfront.

M. Frequency and Quality of Privacy Policy Notices

Of the job sites studied, almost all of the sites had a posted privacy policy. This marks an improvement from 2001, when the sites were last surveyed for policies. Out of 53 sites that made it into the final study, only 5 did not have posted privacy policies.

The policies on the whole tend to be well-fleshed out, and though few adhere to the full OECD guidelines, they are usually full, one-page policies.

Most of the sites studied provided separate links to privacy policies. However, those links could be a challenge to find.

It is a best practice for job sites to link to a privacy policy on the home page of a site, and on every page where job seeker data is collected.

V. Privacy Issues at Specific Job Sites

In the course of research some online sites or businesses raised new or important privacy questions. Each site is discussed in more detail below..

A. USAJOBS.gov and StudentJobs.gov

The federal government's official job site is USAJOBS (www.usajobs.opm.gov) . Its companion site for students is StudentJobs.gov (www.studentjobs.gov).

The USAJOBS site, due to its size and position as the primary gateway for access to federal employment opportunities, is of vital public interest. The Office of Personnel Management (OPM) oversees the operation of the two sites.

When researchers analyzed these sites, they realized that the sites were being outsourced in their entirety to Monster.com.

In order to find out more about the operations of these sites, on October 22, 2003 the

Electronic Privacy Information Center (EPIC) submitted a Freedom of Information Act request to OPM's FOIA Officer by Fax and mail. The FOIA letter requests copies of all documents, electronic and otherwise, pertaining to USAJOBS and the Recruitment One-Stop project, including copies of all contracts regarding USAJOBS.

B. FastWeb.com

FastWeb's use of EEO-related data was discussed earlier in this report under the heading "Use of EEO and ADA Information Online."

Research additionally found that FastWeb has a generous opt-in/data -sharing policy in its privacy policy. The policy states that upon user opt-in, FastWeb has the ability to share consumer data with third parties, including with potential employers. This is fairly straightforward.

"If you give your permission to allow third parties to contact you, personal information about you (such as your contact information and other information collected during your visit to FastWeb) may be shared with colleges, universities, potential employers, recruiters/headhunters, data aggregators, marketers (possibly in the form of list rental), and other organizations. Regardless of your decision regarding the sharing of your personal information, we may share broad aggregate demographic data and related usage information with our business partners."²⁶

If a student opts in to the data sharing, then the student has agreed to the terms above, among the others located in the full policy.

On the "Student Activities" page part of the FastWeb questionnaire, students were asked to "select all that apply" regarding student disability/illnesses. Disabilities/illnesses students could select if applicable included:

- HIV-related
- Multiple Sclerosis
- Emotional
- Deaf/Hard of Hearing

Under "Student Activities, Skills, and Other" students were again instructed to select all that apply. Choices included everything from "Cheerleader" to "Gay/Lesbian" to "Fraternity Member."

If the terms of the privacy policy were strictly adhered to, FastWeb could conceivably share this data with just about anyone. Given the terms of the privacy policy, FastWeb's inclusion of such highly sensitive personal data raises the question: is data regarding student medical condition and/or sexual preference shared, per the privacy policy?

C. Eliyon

Eliyon is a technology company based in Cambridge, Massachusetts. It has built a

database of more than 16 million executives .²⁷ This database is accessible to and searchable by anyone with a Web connection.²⁸ The database contains detailed profiles on individuals based on information the company garners from the Internet, among other sources. It sells these profiles to marketing companies and to recruiters. Monster.com resells access to the Eliyon database.

When queried about the database, Eliyon responded by writing to researchers the following:

Thank you for contacting us. Eliyon is as concerned about privacy as you and others are.

The information in Eliyon is compiled from public sources that are available to everyone on the Internet. Our system collects only information that was likely put in the public domain as a direct result of an action by the person or the person's representatives. Such action may include a press release about a nomination or a promotion, a bio posted on a "management team" page of a company web site, the person being quoted in an article, mentioned as a speaker in a conference, or other such publicized sources.

Eliyon specifically does not collect "public domain" information that likely was put in the public domain without the person's consent and that might include private personal information such as: court documents, driver license registration, real estate records, criminal records, news groups, postings to private listings, etc. Eliyon's crawlers comply with robots.txt standards, avoids crawling private, password protected, web sites, and does not extract any personal information such as marital status, income, hobbies, criminal records, and such.

Researchers found that the database contained many errors and revealed personal, non-work -related information. For example, it revealed childrens' names in one profile of a parent, along with that person's marital information.

Eliyon does not have a privacy policy or an opt-out mechanism for those profiled. It does not allow people to correct their own profiles if inaccurate information is discovered. Meanwhile, the information is being widely used for recruiting and hiring purposes.

Currently, anyone with a Web connection can log on to Eliyon and search the database by company name. However, a new service is being beta-tested that allows searches by an individual's name.²⁹

Eliyon is urged to post a robust privacy policy that allows users to correct and delete information in their profiles.

VI. Employment Application Kiosks and Sites

Employment kiosks – small, mobile ATM-like booths – are increasingly being used for screening job applicants. The booths are typically located in malls and at the front sections of retail stores. The booths allow job candidates to pull up a chair, answer a series of detailed questions, and apply for work in about an hour. No muss, no fuss, and no resumes are needed to apply.

In place of a resume, many of the employment kiosks that researchers studied requested that job seekers supply SSNs, date of birth, and the answer to detailed skills and personality questions. Some kiosks also facilitated an instant SSN check and instant background check.

The kiosks are usually equipped with a miniature keypad, phone, mini computer screen, and secure connection. But all too frequently, the kiosks do not come equipped with the most important thing of all: a privacy policy that discusses how a job seekers' SSNs, dates of birth, and questionnaire data are stored, handled, and deleted, among other things.

As such, the rapid deployment and adoption of kiosk technology in the retail sector as the de facto means of applying for work represents some risk to the affected job seekers.

Researchers sampled a variety of kiosks. Due to the large size of the kiosk market, researchers focused their efforts on the dominant company in the sector, Unicru, which has evaluated more than 19.5 million candidates through its kiosks and related Web sites. For reasons of practicality, researchers further focused the research on one national retail company that currently uses the Unicru kiosks.

Research found that:

- Unicru kiosks studied did not post privacy policies prior to requiring job applicants to enter SSNs, date of birth, and other highly personal information.
- The Unicru kiosks studied did not post or offer a privacy policy to job applicants at any time before, during, or after the kiosk application process.
- The specific employer researchers tested failed to fully comply with all measures of the withdrawal of electronic consent for a background check.

A. Introduction to the Kiosk Issue

In order to have a meaningful privacy discussion about kiosk issues, it is important to first address some general questions.

1. What companies are using kiosks to screen applicants, and how many kiosks are currently deployed?

Retailers, county and city workforce development centers, staffing firms, and other employers have deployed kiosks. Briefly, by way of example:

- Blockbuster deployed an estimated 4,000 employment kiosks in the year 2000.
- Albertson's deployed an estimated 2,300 kiosks across its retail stores in Feb.,

2003.

- Sports Authority has deployed kiosks in its retail stores nationwide.
- Sears has employment kiosks in its retail stores.
- JobView has deployed at least 200 kiosks.
- Adecco has had at least 50 “jobshop” employment kiosks nationwide.
- Los Angeles County has deployed at least 13 job kiosks.
- Dallas Fort Worth has 40 job kiosks deployed through the DFW employment centers.

According to Kiosk Magazine, as of 2003, an estimated 350,000 kiosks of all types are installed worldwide. In the U.S., the installation base is an estimated 125,000 total kiosks. One kiosk costs approximately \$35,000 and up.

2. Why are kiosks starting to become a standard for job application in retail stores?

Proprietary skill and personality testing is being sold as a way to dramatically reduce retail turnover, and touch screen kiosks are being sold as one of the easiest ways to deploy this testing for applicants. Another factor pushing adoption is the instant background check capabilities of the kiosk systems, which appeals to employers concerned about security.

3. What companies are involved in providing services to this market?

Among the companies providing hardware, software, and proprietary testing services in this market are ERI, NCR (EasyPoint Employment Kiosks) and Unicru. ChoicePoint is among the Consumer Reporting Agencies providing background checking services for kiosk service providers.

4. How does the kiosk application process relate to retailers’ other application processes?

After testing the kiosk systems, researchers found that in many cases, the kiosk precisely mirrors the online or Web application system of the retail store where the kiosk is located.

B. The Role of Unicru in the Kiosk and Retail Job Sector

Unicru, a Beaverton, Oregon company dominates the kiosk space. Unicru says it processes approximately one job application per second during the average U.S. workday. All totalled, Unicru processes about 6 million job applicants per year, and has processed a total of more than 19.5 million candidate applications. In 2002, Unicru achieved record revenues of \$21.1 million and was recognized as one of the fastest-growing companies in the U.S. It says that it is the leading provider of hiring management systems.

Unicru has developed proprietary artificial intelligence programs that it claims reduces turnover for its clients. It deploys its AI programs on "more than 13,000 on-site application centers and Web-based solutions." That is, kiosks and Web sites.

Job seekers fill out the kiosk applications and take the employment tests, which are submitted directly to Unicru. The tests are graded and the applications are categorized into green, yellow, or red. Reds are automatic discards, and do not get to the interview level with employers.

Marriott, Target, CVS, Bennigans, Blockbuster Entertainment, Metro One, Kroger, Albertson's, Acme Markets, Big Y, The Fresh Market, Jewel, Osco Drug, SavOn, A&P, Farm Fresh, Spartan Stores, Sports Authority, Universal Studios, Southeastern Freightlines, are among the companies using Unicru.

Unicru currently, in addition to personality testing, also performs instant online background checks on applicants in the locations researchers tested.

1. Methodology

Because Unicru deploys the largest number of kiosks and has tested millions of employees, and because researchers had physical access to a number of Unicru-driven kiosks, researchers chose to study the Unicru kiosks in detail. Each retail outlet that boasts a Unicru-powered kiosk also has a Unicru-powered Web site. Researchers looked at both mediums.

Researchers, for practical purposes of focusing the study, decided upon Sports Authority kiosks and its associated Web sites to study. Researchers had physical access to four different Sports Authority kiosks. Researchers applied at the kiosks in person, and researchers applied at the online Unicru-driven Sports Authority Web site.

<<http://www.thesportsauthority.com/corp/index.jsp?page=jobs>> .

Researchers applied multiple times, and asked volunteers to apply in other states and report their experiences.

Each screen the researchers saw was recorded and compared with the Sports Authority online site, and was found to be almost identical in terms of the job application process.

After the study was complete, researchers checked the results against other Unicru-powered kiosks at Albertsons retail stores.

2. Where are the Privacy Policies?

The Unicru kiosks at Sports Authority stores did not post privacy policies. The Unicru section of the Sports Authority Web site did not post a privacy policy. (The Sports Authority Web site did have a separate privacy policy for e-commerce shoppers, but it

was not available at the Unicru job application section of the site.)

Specifically, at Sports Authority, a job seeker applying online will not see a privacy policy linked to or available during the job application process. And a job seeker applying at the kiosk in the stores will not see a privacy policy.

No law says that a company must post a privacy policy. But a company that is requesting jobseekers' SSN, date of birth, home phone number, name, residence, employment history, and conducting detailed skills and personality testing would provide great benefit to consumers by providing one.

Unicru, on its corporate Web site, posts a privacy policy. It states that it is a TRUST-e Seal participant. But Unicru does not link to this policy from Sports Authority store kiosks or Web sites.

There is no meaningful way for a job seeker at Sports Authority to read a privacy policy prior to giving up his or her SSN or other data. The principles of Fair information Practices need to arrive at employment kiosks, and quickly.

At the minimum, Unicru and all employers using kiosks should post or provide the following:

- A robust, clearly worded privacy policy that appears on the kiosk screen prior to the point that job seekers are requested to enter any personal data about themselves, including name.
- A clearly posted policy that outlines all of the ways that Unicru and each third party involved in the job application process stores, handles, shares, and deletes user data.
- Written, take-away papers or brochures for job applicants with all relevant contact information for background check companies and any third parties involved in or relevant to the job seekers' transactions with the kiosk.
- Kiosks have become part of the employment infrastructure, particularly for retail workers. This piece of the infrastructure absolutely needs to come into line with Fair Information Practices and provide the highest level of privacy notice, disclosure, and openness to job seekers.

3. Problematic Fair Credit Reporting Act Issues

Researchers physically visited the Unicru-powered kiosks in Sports Authority stores in the San Diego region to check for compliance with the FCRA provisions. In areas outside of San Diego, researchers called each and every store in California and spoke to managers to acquire the information.

Researchers found that the Sports Authority stores with Unicru-powered kiosks do not, practically speaking, provide a meaningful way for job seekers to withdraw electronic consent.

4. What Constitutes Valid Electronic Consumer Authorization for Furnishing a Credit Report?

When job seekers apply at a Unicru kiosk at Sports Authority, they walk through a series of screens in which they agree electronically to allow Edge Information Management to conduct a background check on them. (See Appendix A for the screens.)

The exact wording of these screens is critically important because the Fair Credit Report Act has numerous provisions that protect job seekers in the area of employment background checks. Section 604(a)(2) of the FCRA provides that “any consumer reporting agency may furnish a consumer report in accordance with the written instructions of the consumer to whom it relates.” The translation being, a job seeker needs to give written instructions, or authorization, before a background check may be conducted. An employment background check that is conducted without written authorization is illegal under the FCRA.

In Unicru’s kiosk space and at Unicru-driven Web sites, then, the question of electronic authorization comes into play. Is Unicru getting legitimate authorization for the instant background checks at its kiosks and online application sites?

In 1999, the FTC addressed questions about how to procure adequate consumer authorization for background checking via electronic means. In particular, FTC’s “Landever” staff opinion letter states that a consumer simply making one mouse click on a screen does not constitute adequate electronic consumer consent.

That being said, the FCRA does allow electronic consumer consent in Section 604(b)(2)(B)(ii), which “provides that certain job applicants may authorize a consumer report for employment purposes electronically as well as orally or in writing.”

The FTC further clarified electronic consent to background checks in its Zalenski staff opinion letter regarding the E-SIGN Act Section 101 which gave legal force to electronic signatures. The letter outlined three important issues for job seekers:

1. Whether or not the electronic signature is valid will depend on the specific facts of each situation.
2. The electronic signature must clearly convey the consumer’s instructions.
3. The FTC stated that as specified by Section 101(e) of the E-SIGN Act, that consumer’s electronic authorization “must be in a form that can be retained and retrieved in perceivable form.”

5. Is Unicru compliant with the FCRA regarding electronic consent?

Regarding the validity of Unicru’s electronic consent methodology, it is quite likely that a court proceeding would find that Unicru’s series of questions to job applicants would be construed as valid electronic consent because it involves more than one mouseclick. (Landeaver letter).

Regarding the clarity of the consumer’s instructions, the Unicru kiosks are designed to clearly convey the job seeker intent. This, too, would likely stand up to a legal challenge.

6. Is Unicru providing meaningful opportunity for jobseekers to revoke electronic consent?

One of the Unicru screens states that jobseekers have the right to revoke electronic consent at any time during the application process. The screen then instructs job seekers to contact a store manager or person in charge at the location and sign a “paper Authorization” if they choose to revoke electronic authorization. If a paper application were actually available, Unicru/Sports Authority would be in compliance with the applicable provisions of the FCRA.

But when researchers physically entered the stores and applied for jobs, researchers asked Sports Authority managers for paper authorization forms during the application process. There was not a single instance in which that piece of paper or opportunity was provided to researchers.

Further, while applying at the Unicru-powered Web sites at SportsAuthority.com researchers stopped and called store managers to ask them about getting the authorization in paper form. Researchers were repeatedly told it was only available electronically.

8. Conclusion regarding electronic authorization

If Unicru, Sports Authority, and other companies seeking to conduct instant background checks with electronic authorization at kiosks want to truly comply with all of the provisions of the FCRA, as a practical matter, compliance will need to be “ground truthed” and tested at retail kiosk locations. If a manager is supposed to provide a paper authorization form, those forms should be available.

C. Kiosk Industry Recommendations

- Kiosks and the retailers that use them must prominently post OECD-compliant privacy policies. The privacy policy should cover the third party running the kiosk as well as the retailer handling the applicant data.

- Employers must take responsibility for FCRA compliance.
- If an applicant does not want to apply using an online system, a paper alternative should be readily available to them at each and every retail location with a Unicru-powered kiosk or any other kind of kiosk.
- Employers should provide applicants with a way of printing out and retrieving the information they have supplied to the employer upon request, and they should be told that this is available to them and encouraged to avail themselves of this opportunity.
- The HR-XML consortium needs to re-open its technical background check specifications and fully incorporate the internationally accepted OECD guidelines.

Kiosks are not an inherently negative technology. But without meaningful privacy policies, Kiosks at this time represent a negative development in the job search industry. With the number of kiosks growing rapidly, this is an area that needs to be examined before negative consumer privacy practices become ingrained.

Kiosks, their associated Web sites at retailers, and the retailers themselves need to commit themselves to fully implementing the full Fair Information Principles as outlined by the Internationally agreed upon OECD 1980 guidelines. And if retailers and others are going to use kiosks and associated Web sites that make certain claims about FCRA compliance, they must follow those claims up meaningfully and “groundtruth” compliance.

E. Consumer Tips for Using Employment Kiosks and their Related Web sites

- Do not submit your SSN or date of birth to a kiosk or a Web site that does not have a privacy policy posted prominently prior to the time this information is requested of you. If you do, you truly lose control of this information.
- If you have any arrests or suspended convictions in your background, you may want to think twice about agreeing to an “instant” or “national” background check online. Some (but not all) of these national credit checks that are conducted through accessing proprietary databases online pick up and report information that should not be reported, such as suspended convictions.
- As such, the employer may get information they should not under the FCRA. This is a complex area of the law. ESR maintains a helpful set of articles about pre-employment background screenings.³⁰

- If you have been denied employment based on the results of an instant background check, you should be notified in writing of this adverse decision.
- If an instant background check has been conducted and has found a criminal conviction, the company conducting this check is to report to you that they did the check and reported the findings.
- When you use a kiosk to apply for employment, bring a pencil or pen with you so you can write down all contact information that you are given at the kiosk regarding a background check or your application.

VII. Privacy Practices at Resume Distribution Services

Resume distribution services send job seekers' resumes to a mix of recruiters, job sites, and corporations, with recipients typically numbering anywhere from dozens of recipients to several hundred. Most major job sites such as Monster.com, FigureJobs.com, and others have some sort of affiliation or links to a resume distribution service. Some sites, such as JobBankUSA.com, run their own service. Resume distribution sites have been both reviled and celebrated, depending on the expert discussing them.

After testing the distribution sites and conducting test resume distributions, research has found that the resume distribution services raise some consumer privacy issues.

Some of the key issues at these sites include:

- May a consumer check – before purchase – what individuals or businesses will receive the resumes?
- How may a consumer validate the person or company receiving the resumes? Is there a link to the recipients' sites, or full contact information?
- Can consumers choose at the time of purchase which specific members of the list are to receive the resumes, while deselecting others?
- If there are problems arising from the mass distribution, how can a consumer adequately resolve those problems?

Some resume distribution sites advertise heavily to jobseekers via emails. Many job seekers therefore know about these sites, but few understand how they really work before using them. Because of distribution sites' increasing presence, this study seeks to learn more about these sites and to shed light on their consumer practices.

Researchers selected key sites, looked at their privacy, security, and business practices, and conducted test "blasts" of resumes. Research indicates that job seekers who use these

sites may have an excellent experience, or may have their personal information get out of their control.

A. Results

Results of site testing revealed a cluster of issues surrounding the distribution list members. There is a general lack of security regarding who could sign up to get on the sites' resume recipient lists. Frequently, researchers could not adequately validate the list members prior to purchasing services. One of the lists that allowed prior verification revealed questionable list members.

Additional issues were weak to non-existent privacy policies, BBB seal fraud, and some sites' aggressive affiliate marketing programs.

B. Lack of Security in the Sign-Up Process

Of the sites studied, almost every site allowed recruiters to sign up to receive resumes free of charge. This policy encourages large numbers of recruiters to sign up for the services. However, some but not all sites appear to have little meaningful validation in vetting these recruiters.

In order to test the privacy and security of the system, researchers attempted to sign up to receive resumes. All it took was filling out a form on a Web site to land on the receiving end of a resume distribution list. Researchers listed their real company name, real company hiring needs, a real phone number, and an e-mail address. Without any sort of vetting or clearance, researchers were approved to receive candidate resumes.

The researchers adhered to the Terms of Use in their signup, and as soon as they were able to substantiate that they successfully got on the list, they took themselves off of the lists.

It is disturbing that anyone can sign up to get these resumes. Job seekers pay a between \$35 to \$150 to send out a single resume. But to whom are these resumes going?

C. Who gets the resumes?

One of the serious questions these services raise is that not every site publishes the complete list of companies and individuals receiving the resumes. This is problematic, because as already discussed, in most cases it is incredibly simple to sign up to be a resume recipient. However, some sites do publish their lists.

Some examples illustrate the scope of this situation.

- ResumeRabbit lists the job sites it sends resumes to, and links to the sites. This is a first positive step for consumers to be able check to see if the recipients are legitimate.

- ResumeViper is another site that provides its list prior to purchase. However, the list is questionable. It consists of thousands of individuals and companies.³¹ In a close look at the law enforcement employer section of the list, on October 17, 2003, researchers found a company called “Paid Response.” This company was listed as employer number 108. This company, according to its Website, hires home “ad typist” workers. Is this a valid law enforcement employer hiring for a security position?³² Number eight on the list of law enforcement and security employers was Alya, Inc. Alya is the corporate name of ResumeViper.³³ Again, is this a valid law enforcement company or employer?
- One service that researchers paid to test, ResumeDirector, did not reveal the distribution list members prior to purchase. However, after purchasing the service and before sending the resume out, researchers were able to select exactly what job site received the resume on a Web site form.
- ResumeXposure, another service researchers paid to test, did not reveal its list of distribution members before purchase. It also did not reveal its list before the resume was sent out. After the resume was sent, researchers received a list of recruiters who had received the resume. That being said, researchers received two legitimate job offers after using the service, and almost zero spam.

Ideally, consumers who use these services should see exactly who is getting their resume prior to making a purchase decision. The list should be accurate, and consumers should be able to choose who does and does not get the resume before it gets sent out. In this age of identity theft and job scams, sending resumes out to an unnamed or unclear cast of thousands is not for the weak-hearted.

D. Privacy policies at resume distribution sites

Of the sites that did have privacy policies, researchers found that the policies were sometimes incomplete, and did not fully disclose site practices.

The policies that were more complete tended to contain many loopholes and caveats in the area of marketing and the use of consumer emails in particular. Some of the policies that were well-written in some cases documented negative consumer practices.

For example, ResumeRabbit disclosed in its privacy policy that it tracked and profiled customers’ reading, viewing, and Web surfing habits without directly asking customers for that information.³⁴ This is broadly known as “profiling,” and is viewed as a negative privacy practice. While it is positive that the site disclosed this practice, the practice itself is negative.

On the positive side, one site, ResumeDirector, did have a resume deletion policy, which was rare to find. Another positive practice for consumers at the sites with privacy policies is that most of them disclosed credit card security practices, with most using

some form of secure transmission.

E. BBB Reliability Seal Program Issues

The BBB Reliability Seal program is a consumer program meant to help protect consumers from online fraud. Consumers, if faced with insurmountable problems with a business, may file a complaint about member companies, and may also seek arbitration through the BBB.

At the time this report was prepared, some of the sites were displaying a BBB seal incorrectly. It is positive that some of the sites were participating in a Seal Program. But the fraudulent use of the seal by in some cases prominent companies is problematic both from a privacy and a business standpoint.

In this sector where making an informed choice is challenging for consumers, the BBB Seal has high value. As part of this report, researchers wrote a letter to the BBB notifying them of the broken seals. At the time of publication, the BBB had already taken action to begin correcting the broken seal issues.

F. Specific Seal Issues

At the time of this writing, the specific sites displaying a BBB Reliability seal incorrectly are as follows:

- Resume.com deactivated its seal links on its home page and on its privacy policy page, but still kept the seal up.³⁵
- ResumeViper had a non-linked BBB Online Safe Shopping Site Seal on its home page. The ResumeViper privacy policy page, however, had a seal that linked actively to a BBB search site.³⁶

G. The impact of “affiliate marketing partners” on consumers

Many resume distribution sites encourage people to become a marketing affiliate and earn money by referring visitors to their respective sites. ResumeRabbit’s affiliate program, as of February 20, 2002, numbered above 1,500 members and generated substantial revenue for the company.³⁷ ResumeRabbit said it pays its affiliates \$20 for each sale.³⁸ ResumeViper pays up to 30% commission on every sale generated through a referral,³⁹ and ResumeXposure pays \$25 per referral.⁴⁰ Other sites with referable programs include ResumeDirector, e-Resume.net, ResumeZapper, BlastmyResume.com, and ResumeGator – to mention a few.

According to ResumeXposure’s numbers, employment-related sites average 1 sale for every 50 to 100 clicks, with the average earnings per click at about 22 to 45 cents per

click.⁴¹ No wonder, then, that Web sites list resume affiliate linking opportunities, and discuss affiliate marketing as a viable way to make a profit on the Web.⁴²

Researchers, after posting resumes on numerous job sites, received many emails asking them to visit various resume distribution sites. Many of these emails were from affiliates using potentially unfair and deceptive marketing practices to get “click throughs.”

For example, some affiliate marketing emails were written to look like they came from recruiters. When researchers clicked on the links in the emails to test them, the referring URL from the email gave the affiliate information to the resume distribution site. If a sale had occurred from this click, the emailer would have earned some money from researchers’ clicks.

H. Site by Site Results

Resume Director (HireResume, Inc.)

www.resumedirector.com

Privacy policy: Yes

BBB Online Safe Shopping Site Seal member in good standing.

ResumeDirector’s privacy policy covered many of the 8 principles in the Fair Information Practices guidelines. Researchers chose to use ResumeDirector for a distribution test based on the relative strength of the privacy policy, and because of its BBB membership and good record.

ResumeXposure.com

www.resumexposure.com

Privacy policy: Yes.

0 complaints to BBB during membership, active BBB member.

ResumeXposure.com is an active BBB member and has no complaints on record. The Terms of Use⁴³ on the site are very good, and follow the security principle of the Fair Information Practices.

Rocket Resume

www.rocketresume.com

Privacy policy: Yes

BlastMyResume

www.blastmyresume.com

Privacy policy: yes

Resume.com

www.resume.com

Privacy policy: yes

BBB Online Safe Shopping Site Seal violation

ResumeRabbit

www.resumerabbit.com

Privacy policy: Yes

Valid BBB Seal.

ResumeRabbit is a member of the BBB Online Safe Shopping Site Seal program..

Resume Catapult

www.resumecatapult.com

Privacy policy: yes

Note: refund policy also available

Resume Catapult's privacy policy adhered fairly well to the principles of Fair Information Practices. The site has a rare refund policy on the site, which is positive for consumers.

Resume Blaster

www.resumeblaster.com

Privacy policy: No

BBB Online Safe Shopping Site Seal is expired.

ResumeBlaster is a safe shopping seal participant, but at the time of research the seal had expired.

ResumeXPRESS

www.resumexpress.com

Privacy policy: No. (See Note)

Affiliated with 6Figurejobs, Allen and Associates, and others.

Note: On the customer sign up page ResumeXPRESS lists a Terms of Use. This terms of use mentions a privacy policy, but does not provide a link to it.

ResumeBroadcaster

www.resumebroadcaster.com

(Job Bank USA.com, Inc.)

Privacy policy: No

Active BBB Online Safe Shopping Site Seal (see note)

Note: As of October 16, 2003, the site did not have a privacy policy; this violates the BBB Seal program.

ResumeViper (Alya, Inc.)

www.resumeviper.com

Privacy policy: Yes

Improper BBB Seal display

As of October 16, 2003, ResumeViper was displaying an invalid BBB Online Safe Shopping Site Seal on its home page and other pages of its site.

I. Industry Recommendations

- Resume distribution sites should conspicuously post clearly worded privacy policies that reflect all of the eight principles of Fair Information Practices. Privacy policies should ideally be linked separately, and the privacy policy should not be a challenge for consumers to find.
- Resume broadcasters should set up safeguards and checks to carefully validate each person or business that signs up to receive resumes.
- Resume distribution sites should make available to job seekers a complete, accurate, and up-to-date list of each business, employer, or individual that will receive the distributed resumes and make that list available to consumers prior to the point of purchase.
- Resume distribution services should provide a simple, effective way for job seekers to validate each and every entity on the resume distribution list.
- Affiliate and marketing partners should be chosen carefully, and should be required to abide by fair business practices in their solicitations to job seekers.
- It is a best practice of resume distribution sites to test their own systems regularly to see what companies are sending job seekers spam and inappropriate email.
- Sites with broken seals should either become a member in good standing, or remove the seals from their sites.

J. Consumer Tips for Using Resume Distribution Services

- It can be very challenging to make a good choice about which service to use. Here are tips to help you.
- If you do not see a privacy policy posted at a resume distribution site, think twice before using the site. A privacy policy is a legal document, enforceable by the Federal Trade Commission. It does give you some protection.
- Things to look for in the privacy policy include credit card encryption, resume deletion, refund policy, and marketing policy.
 - a. The privacy policy should state that it protects your credit card transaction. The term to look for is “SSL,” or “encryption.”
 - b. The policy should state how you might delete your resume.
 - c. The policy should state what the site does with your information. Does it sell or share your information? Does it share your information with marketing or advertising companies?
 - d. The policy should state how and under what circumstances you could get a refund if you are unsatisfied with the results of the service.

- If finding the privacy policy is a lot of work, treat this as a red flag. Look for privacy policies that are clearly and conspicuously posted on every single page of the site.
- If you can't see a complete and accurate list of the people and businesses that will receive your resume before you pay for the services, you should not use the site. Would you buy a pair of sunglasses or jeans that you had never seen or tried on before? It's no different with these distribution sites.
- A BBB Seal on the site is positive, but only if it works. Many people see a BBB Seal on a site and take it at face value. Our research found that many of the sites that had seals either weren't real members of the program, or that the site was breaking the rules of the seal program.

VIII. Privacy Practices at Resume Writing Services

Resume writing services exist to help jobseekers create a portrait of their skills and work experience that is compelling enough to land the job seekers interviews for desirable positions. These types of businesses tend to be small one to 35- person operations. Data privacy has arrived in this corner of the job search universe; resumes containing rich data such as work history, name, address, phone number, e-mail address, and educational history are prime treasures in the data business.⁴⁴

In the course of the job search study, researchers discovered a site that stated outright that it purchased resumes from resume writing services.⁴⁵ This site, HotResumes.com, also sold resumes without the knowledge of the resume owners. An invoice for the sale of over 4,900 resumes is available as proof of this sale.⁴⁶

Because of the disturbing questions raised by the HotResumes.com statements on its Web site, and the fact that the HotResume site sold job seeker resumes, it has become important to consider the resume-writing segment of the job search industry for its privacy practices.

The resume writing business is an area where honor has ruled for decades. Most of these businesses would not dream of selling resume data. But those past days of data innocence where job seekers simply relied upon implicit trust of resume handling practices are very much gone. Privacy policies posted prominently on Web sites, which form a legal basis of trust prior to a customer's purchase, are more appropriate in today's data environment.

Research found that:

- Over half of the businesses posted a privacy policy, yet nearly all accepted some form of credit card payment.

- The privacy policies that were posted were generally incomplete according to OECD guidelines. A few but not all privacy policies stated outright that the business would not share or sell resumes to third parties.
- 2 of the 20 businesses were valid, up- to- date members of an e-commerce seal program.
- When contacted by email with a consumer privacy question, 12 out of 20 sites responded to the query. One business said that it deleted the email because it thought the query was spam. Of those that responded to the query, all of the businesses were forthright about stating privacy goals and standards and provided excellent privacy statements to consumers.

A. Introduction

Resume writers charge fees ranging from about \$50 to over \$800 per resume. The lowest average cost for what is considered a quality rewrite is at least \$250 - \$400, with \$250 being considered a rock-bottom price. For government jobs, it is rare to pay less than \$500 to \$800 per resume. Likewise, executives can expect to pay \$500 on up for a professional resume rewrite

Resume writers may be members of a number of professional organizations and may also hold a number of certificates, such as the CPRW or Certified Professional Resume Writer certificate. The professional resume writers' organizations and certification programs are focused on training the resume writers. In terms of professional quality, these groups and certifications have served consumers well. The larger of the organizations have a code of ethics; however, these organizations do not actively enforce or mandate OECD guidelines or the full eight principles of Fair Information Practices for resume writing businesses.

This is important because of the contemporary data environment and also because resume writing services are shifting into a higher profile in general. Resume writing services are frequently pitched to consumers who are looking for jobs using commercial online services. Many online job sites and job-related organizations have some sort of affiliation or partnership with one or more resume writing services, and feature them on their respective sites in a variety of ways. For example, Net-Temps.com partners with Employment911. CareerBuilder partners with e-Resume.net.

The question of which business to choose in this category is particularly important – and challenging -- for consumers. After a consumer hires a resume writing service and makes payment for services, that service will have access to some form of financial or credit card data, the address, real name, work history, and e-mail address of the person using their services. This represents a lot of data, and in an era of identity theft, it is critically important for consumers to have up-front, legally binding assurances about how the businesses will control this information. This translates to having a robust privacy policy posted on the Web site and shared in writing with consumers prior to the point of sale.

B. Privacy Policies on Resume Writing Service Sites

Well over half of the resume writing services studied posted privacy policies on their Web sites. It is perfectly legal for a business based in the United States to operate without having a posted privacy policy. However, consumers are increasingly advised not to frequent a business without a posted privacy policy when that business handles personal and or financial data. If a Web site does not have a privacy policy it does not necessarily mean that the business has poor privacy practices. However, a consumer would not know this, and would not have the legal protection a posted privacy policy assures.

The FTC stated as one of its goals that businesses with Web sites post privacy policies on their Web sites. In its Privacy Agenda statement, the FTC specifically has stated that:

“The FTC has encouraged web sites to post privacy notices and honor the promises in them. Many web sites - indeed, almost all the top100 sites - now post their privacy policies.”

It is a key consumer protection to post privacy policies on business Web sites when personal data is involved.

Writing services with privacy policies on their Web sites include:

10 Minute Resume
CareerPerfect
CareerPro (RezCoach) (Statement of confidentiality available on site prior to notification; after notification, posted a more robust privacy policy.)
Competitive-Edge-Resumes (Posted after notification.)
Employment911 (Policy is located in Terms of Use).
e-resume.net (Policy is located in Terms of Use).
Guaranteed Resumes (BBB Reliability Seal in good standing)
Pathwinner.com
Resume.com
Resume Edge
Resumagic
ResumeWriters.com (Policy is located in Terms of Use).
The ResumePlace (Posted after notification)

Resume writing services with no posted privacy policies on their Web sites include:

Acorn Career Counseling and Resume Writing
Associated Resume Writers (FedJobs)
CareerChannels
CareerPro Resumes
Career-Resumes (Up to date BBB Seal)
Competitive Edge
Successful Resumes

C. Resume Writing Services' Response to Privacy Query

Researchers emailed 20 resume writing services with a basic privacy query. The email was sent one time, and asked if the site had a privacy policy, and asked if resumes were ever shared or sold to others. The queries were sent October 22, 2003 to the contact email address listed for each site. The queries were sent from an email address not connected to any researchers' names or domains. The email was sent in ASCII format, did not contain

any coding or executables, and therefore was not a virus threat.

When a privacy policy was available, the contact information in the privacy policy was used. If not, the most prominent contact information was used. One email was sent out to the listed address posted on the business Web site.

The goal of this query was to see how each site responded to consumer privacy concerns, and to see how or if a job seeker could use these services while still maintaining their privacy with a business they did not yet know. The goal was also, in the case where there was no privacy policy, to see if the sites would give a consumer guarantee of privacy which would suffice in its place. In fact, all of the sites that responded did just that.

Sites that responded to the privacy query said definitively in their emails that they would not sell or share resumes. These sites included:

Career-Resumes.com

Employment 911

Resume Writers.com responded to the query with: "Privacy is guaranteed. This e-mail will stand as proof."

A Competitive Edge

Competitive-Edge-Resumes

CareerPro (RezCoach)

Career Pro Resumes

Successful Resumes

Associated Resume Writers responded with an affirmative statement: "We keep everything confidential and you will be the only one to receive your resume."

e-Resume.net

The Resume Place, Inc.

Sites that did not respond to the emailed privacy query included:

Resume Edge (CyberEdit)*

Resumagic

Careerperfect

CareerChannels (Bridgeman)

Resume.com

PathWinner.com

Guaranteed Resumes (gresumes)

10 Minute Resume

Acorn Center

*Resume Edge Vendor Response: Resume Edge is following up with the customer service department of its site to find out why the privacy query went unanswered. It is ResumeEdge's policy to answer privacy queries.

D. Best Practices Among the Sites Studied

Within the job search industry as a whole, the job search sites do lead the pack in terms of privacy sophistication. These sites, especially the larger sites, have access to legal counsel and are up to date on current best practices in privacy. Many of their policies reflect this knowledge.

Resume writers as a group appear to care deeply about privacy. Yet regarding the current legal doctrines and international guidelines and frameworks, many are just now

beginning to translate their established practices to robust consumer notice and the other principles of fair information practices.

There are sites already displaying best practices that are positive for consumers and represent the best practices in the industry to date.

1. Unequivocal privacy statements regarding resume sharing and selling.

If a privacy policy doesn't specifically state that a resume writing service will not sell or share resumes, then the policy is not as useful as it could be for the job seekers using these services, or trying to choose a service. A policy doesn't have to be fancy; it just needs to be clear. ResumeWriters.com's privacy policy, for example, did not say a lot, but it said the most important thing. It clearly and unequivocally stated in language a reasonable person could easily understand that the site will not sell resumes or resume information.

"We ask for and require certain personal and identification information in order to operate ResumeWriters.com. At no time, and under no circumstances will ResumeWriters.com distribute, disseminate, sell, or disclose any personal or identification information given to us by our customers for the purposes of writing their resumes. Any personal data that is acquired or stored by ResumeWriters.com is for resume writing purposes only. ResumeWriters.com will not store, distribute, disseminate, sell, or disclose the content of any resume writing we receive at our service."⁴⁷

This kind of clear, direct statement constitutes a best practice for resume writing services. This privacy notice, in combination with ResumeWriters.com's clear response to the consumer privacy query provides excellent assurance for consumers who are seeking to protect their data from unauthorized disclosure of any kind.

Another site with a clear, direct and very positive statement about privacy is The Resume Place. When researchers initially approached this business, it did not have a posted privacy policy on its Web site. Yet this business had posted very clear privacy policies elsewhere and had responded very positively to consumer queries. This business is an example of a service that had excellent practices, but just had not posted a policy on the Web site yet.

This business took its existing clear "paper" privacy policy and simply posted that policy on its Web site, with a very clear statement that they would never sell or share resumes without permission. This is an excellent example of a resume writing service with good practices simply stating those practices to consumers.

Because a privacy policy is a legal document, it is the first step in building consumer trust.

2. Anonymous Payment

It is a positive practice for resume writing services to allow payment to be made

anonymously. This provides consumers who are interested in protecting their privacy to use pseudonyms on their resumes and thus remain essentially anonymous to the resume writer.

Pathwinner.com allows users to pay by using PayPal, which is privacy-friendly and is a forward-looking positive practice for resume writing services to adopt.⁴⁸ Resume writers typically want to talk in depth with each person who gives them their resume. While this may be necessary, it doesn't have to be done with a job candidate's real name and address to be done effectively. It does not always serve job seekers to have to give up all of their personal details to a resume writing service, particularly in the case of very high profile executives who may be very privacy-sensitive.

PayPal or other anonymous payment options allow those job seekers who want to retain anonymity the ability to do so.

3. BBB Membership and Seal Membership

For businesses new to privacy issues, an online seal membership program is a positive step toward getting some kind of privacy policy vetting and counseling at a respectively low cost. In the case of a BBB membership, it also gives consumers the ability to look up a resume writing service's track record, which is also positive.

Guaranteed Resumes is a resume writing service that stood out because of its valid BBB Reliability seal posted on its site. This is quite rare among the resume writing services. Another site with an up-to-date BBB Seal is Career-Resumes. The Resume-Place has posted its standard BBB membership in its Web policy, which is another good practice.

E. Privacy Issues at Resume Writing Businesses

Problems in this niche fell into several well-defined categories.

1. Privacy Language Embedded in a Terms of Use

A separately linked privacy policy is a defacto standard. It is not a legal standard, however.

It is arguable that a Terms of Use is not the ideal place to put a privacy policy, though this is definitely a grey area. A Terms of Use is a place where a job seeker may expect to find warrantee information and disclaimers. A privacy policy is, or should be, a separate matter and should ideally focus on how the business handles consumer data.

It is a best practice to separate the privacy policy from the Terms of Use and to treat these documents as separate links on a Web site. That way, consumers may easily and quickly find the privacy statement.

2. Broken Seals on Sites

It is a negative consumer practice to incorrectly display BBB or TRUST-e seals on a Web site. Resume Edge is a CyberEdit company, which is a division of Peterson's, which is a division of Thomsons.⁴⁹ Resume Edge is unique in that it is the only site among the 22 studied that had both a BBB Privacy Seal and a Reliability Seal, which is positive. However, both seals were broken when researchers initially studied the site. *

* Resume Edge Vendor response: Resume Edge, in its response to this report, has taken down the invalid seals, and has stated that it will be following up on this issue immediately. Resume Edge has been in transition, as it has recently been acquired by Thomsons.

The Career-Resumes BBB seal was up to date and valid. It is positive that Career-Resumes has this seal. Ideally, the BBB Seal is to be displayed only with a posted privacy policy, according to the BBB Guidelines.⁵⁰ To make this seal as valid as possible, a privacy policy should be posted, according to the BBB.⁵¹

3. No Posted Privacy Policy on Web Site

Some resume writing services did not have privacy policies posted on their business Web sites. This is not illegal in any way. However, it is a very positive consumer practice – especially when dealing with the combination of personal information and credit card numbers – to post a policy on the business Web site, as the FTC has indicated.

The days of implicit trust in the job search industry are by and large in the past. It is unfortunate, but true.

F. Industry recommendations for Resume Writers

- The professional organizations for resume writers are in a position to greatly benefit their members and job seekers by taking a firm stand on the privacy issue and by encouraging adoption of the full 8 principles of the OECD guidelines by members. The current codes of business ethics for these organizations⁵² are positive, but they could be even more so by incorporating this information. We urge that the professional organizations for resume writers draw up guidelines for their members regarding the internationally accepted privacy standards in cooperation with a coalition of privacy, consumer rights, and employment groups.
- Given the sensitive nature of resume data, all resume writing services should be posting privacy policies on their Web sites. Consumers are becoming increasingly reluctant to engage in electronic commerce without the benefit of a privacy policy or written assurances about what happens to their personal and financial information. Additionally, a posted privacy policy helps to communicate a

businesses' privacy quality. If a business already has good privacy practices, a policy on its Web site will communicate these practices to the consumer.

- The privacy policies should be linked to conspicuously and clearly from each page, if at all possible.
- The privacy policies should be clear, and not contain terms that require law degrees to correctly decipher.
- Resume writing services should affirmatively and clearly state, without conditions except for valid law enforcement, that the site does not and will not share or sell resumes.
- The OECD has an excellent, free privacy policy generator.⁵³ Resume writing services, especially those new to the principles of Fair Information Practices, may find benefit from walking through this tool and seeing where the privacy bar is in terms of the most current and generally accepted practices.
- Resume data combined with credit card data is extremely sensitive. A bright, clear line needs to be drawn on this issue of consumer resume privacy.

G. Consumer Tips for Using Resume Writing Services

- If you do not see a privacy policy posted at a resume writing service Web site, you should think very carefully before deciding to use the site. A privacy policy is a legal document, and it is enforceable. It does give you some legal protection.
- Things to look for in the privacy policy include credit card encryption, refund policy, and an explicit statement about resume sharing.
- The privacy policy should state that it protects your credit card transaction. The term to look for is “SSL,” or “encryption.”
- The policy should state that the business would not share, distribute, or sell your resume.
- The policy should state how and under what circumstances you could get a refund if you are unsatisfied with the results of the service.
- If finding the privacy policy is a lot of work, treat this as a red flag. Look for privacy policies that are clearly and conspicuously posted on the business Web site. The FTC has strongly encouraged all businesses to post company privacy policies on the company Web site.
- If a business allows you to pay with PayPal, take it up on the offer, as it gives you more ability to keep your credit card information private.
- Here is a checklist of the things you can look at to help you make a decision about the quality of the site:
 - a. Does the site have a privacy policy?
 - b. Does the site have secure credit card payment?

- c. Does the site give you a guarantee or warrantee before you buy?
- d. Does the site ask overly intrusive questions? For example, does the site ask for mother's maiden name, bank account numbers, or your physical characteristics? No resume writer needs this information from you, and valid resume writing businesses will not ask for this information.
- e. Does the site ask for date of birth or your Social Security Number? If it does, you should not use the site, and you should report it to the FTC (1-877-FTC-HELP).
- f. Does the site have adequate and correct contact information listed for it? Have you tested the contact information?
- g. Does the site belong to a Better Business Bureau? Have you checked the appropriate BBB for complaints against the business? Does the site post an online BBB Seal? If so, is it a valid seal?
- h. If you send a privacy query to the site, does it answer with an affirmative response to you? You should not have to give up your phone number or address to a business you do not know in order to get a valid response to your questions.

VIII. Best Practices for Job and Career-Related Sites

- **Clear, conspicuous, and abundant posting of a privacy policy.** Fair Information Practices dictate that privacy policies should be posted at or before data is requested of a job applicant or site visitor. And the policies should be posted at every page information is requested of a job seeker.
- **Apply Title VII of the Civil Rights Act vigorously.** Don't hide behind new technologies that allow for an "end run" around the precise stipulations of this critically important standard. While it is possible for sites to get around Title VII issues today due to "targeting" technologies, it is not desirable whatsoever on a societal or individual level. Every site must state voluntary submission of Title VII data, and must keep that data separate from applications – even if that data is submitted electronically.
- **Use of session cookies only.** Some of the largest sites on the Internet, such as Amazon.com, use session cookies only. There is no intrinsic need for job sites to be allowing long-term cookies from their sites or from third parties.
- **Follow the NAI Agreements.** If third party advertisers are allowed to deposit cookies on visitors' computers, then link to that advertisers opt-out cookie, or the NAI agreement page, if applicable. If a third party advertiser wants to deposit a cookie that does not allow opting out, don't use that advertiser.

- **Resume posting areas should be off-limits to advertisers and other third parties.** This is especially true if the site is using GET commands or putting any information that reveals an applicant has posted a resume on a site in a URL where a third party can pick it up using simple computer coding. This is an unfair monetization of job seeker activities on job sites. Job seekers should have the right to look at job ads and post resumes without sharing that information with advertising companies or other non-employment related third parties present on the site.
- **Use the OECD privacy policy generator to check compliance level.** Even if you already have a privacy policy, you can use this tool to check your privacy policy for full compliance with and inclusion of each of the 8 internationally accepted principles of Fair Information Practices. The OECD principles have an excellent balance of free flow of information and privacy protection.
- **Re-evaluate Affiliate Marketing Policies.** If affiliate marketing is available, consider vetting those who market the site and creating a code of conduct for them. For example, sending deceptive e-mails to job applicants is a good thing to prohibit.
- **Use clear, direct wording in privacy policies.** Tricky privacy policy wording will eventually catch up with a business. A cleverly worded policy may allow a site or business to sell or share applicant data without too many applicants catching on. However, someone somewhere will catch on, and then the loss of consumer trust is very challenging to regain.
- **Don't use offline data sources to correlate information in the resume database or email contact list.** Even if you disclose this practice, it is a highly negative consumer practice.
- **Prior to adopting industry standards, involve and solicit meaningful input from a coalition of privacy, consumer advocacy, and labor organizations.** Too often technical and other industry standards have been developed with little to no input from a broad coalition that allows for supporting consumer and broader labor interests.
- **Guard fairness standards in the modern job search.** While sites may well exist to make a profit, there is another much larger and more significant side of the story; that is, a job search infrastructure must be fair and must be experienced as fair by the job seekers who are forced to use it.

X. Consumer Guide to Online Job Sites

How to read and understand the site results

Each site underwent extensive testing. The results of the testing are listed under each site. For general consumer tips about job searching online, please see heading, “Consumer Tips for Job Searching Online.”

Here are explanations of each item in the site listing:

- **Privacy policy:** This indicates if a site has a posted privacy policy on its Web site. A privacy policy is a legal document that will indicate to you how a company will use and handle your personal data.
- **Registration required/not required:** This tells you if you have to register and give your personal information before you may look at job ads.
- **Deposits third party session cookies:** This means that the site will put information on your computer from companies other than the site you are visiting. The information will last on your computer until you close your browser, or for one browsing “session.”
- **Deposits short term third party cookies:** This means that the site will put information on your computer from companies other than the site you are visiting. This information is short-term and will expire sometime between a day to a month or two.
- **Deposits persistent third party cookies:** This means the site you are visiting will put information on your computer from companies other than the site you are visiting. This information will be on your computer for anywhere from 6 months to decades, unless you erase it or do not accept it in the first place.
- **0 third party cookies:** this means the site will not put cookies belonging to another company on your computer when you visit the site.
- **Persistent cookies from site:** This means that the site you are navigating to will place its own cookies, or information, on your computer. This information will last anywhere from six months up to a decade or more unless you delete it.
- **Site responded to privacy query:** This means that when researchers sent a consumer question about privacy to the site via email, that the site either did or did not answer the email.
- **Site allows use of anonymizing services:** If a site supports or allows anonymizing services, it means you can use the site without revealing your identity at all. Anonymizing services include use of proxies, like the Junkbuster proxy < <http://www.junkbuster.com/>> or free/pay services such as @anonymouse < <http://anonymouse.ws/>> and Anonymizer.com < <http://www.anonymizer.com/>>

> . Anonymizer.com has a free privacy test you can take to see what your Internet browser is revealing when you visit Web pages. All you do is visit the URL, and it will tell you what it sees:

<<http://www.anonymizer.com/privacytest/index.shtml>>

- **Resume posting resulted in:** This lets you know what happened to researchers' test resumes. All of the resumes were posted openly, not confidentially. This means that the resumes received maximum exposure, which is what most job seekers choose when posting resumes. If a marketing statement (we will send you information about our site) was automatically selected, we left it selected. Researchers opted in to receive marketing information from the site if it was not already done for them.
- Occasionally, some sites have additional notes. For example, if SSN is requested at the site, we list this.

Important Consumer Tips to remember when accessing online sites:

- No matter what site you access, you should always be extremely careful about giving out your SSN, date of birth, gender, race, and any sensitive medical or personal information.
- Title VII of the Civil Rights Act of 1964 < <http://www.eeoc.gov/laws/vii.html>> prohibits companies from discriminating against you based on race, color, religion, sex, or national origin. Some Web sites will ask you to specify your gender and/or your race to help companies comply with this law. Providing this information is voluntary.
- There is never a circumstance in which you should give an employer or Web site your credit card number, your bank account information, plus your SSN and date of birth. Valid employers will not ask for a credit card number or a bank account number, even to conduct a background check. For more details about this topic, please see the Consumer Tips section.

6 Figure Jobs

www.6figurejobs.com

Privacy policy: Yes

No registration prior to looking at job ads

Deposits third party persistent cookies

valueclick.net exp. 2028

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

*Note: not all resumes are accepted for inclusion in the resume database.

To opt out of the ValueClick Opt tracking cookie, check here:

<http://www.valueclick.com/privacy.html>
Scroll to mid page and look for the link that says "Click here to go to Opt Out page."

Adecco

www.adeccojobs.com

Privacy policy: Yes
No registration prior to looking at job ads
0 third party cookies of any type
Site did not respond to privacy query
Site allows use of anonymizing services
Resume posting resulted in 0 spam from third parties

Americas Job Bank

www.ajb.dni.us

Privacy policy: Yes
No registration prior to looking at job ads
0 third party cookies of any kind
Site responded to privacy query
Anonymizing services do not work well at this site

BestJobsUSA

www.bestjobsusa.com

Privacy policy: Yes
No registration prior to looking at job ads
Site did not respond to privacy query
Site allows use of anonymizing services
Present on site:
 Superstats
 Mycomputer.com
You need to accept cookies to use this site
Resume posting resulted in 0 spam from third parties

Black Collegian

www.blackcollegian.com

Privacy policy: Yes
No registration required prior to looking at job ads
0 third party cookies of any kind
Site responded to privacy query
Site allows use of anonymizing services
Resume posting resulted in 0 spam from third parties

BrassRing

www.brassring.com

Privacy policy: Yes
No registration required prior to looking at job ads
Deposits third party persistent cookies from:
 imrworldwide exp. 2009

Site did not respond to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

Please note that job ads at BrassRing are hosted at CareerBuilder.

For more information about IMRWorldwide cookies, please see: http://www.redsheriff.com/us/content/products_1_1.html

CaliforniaJobs.com

www.localcareers.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits third party persistent cookies from

Fastclick.net: exp. 2005

Deposits persistent cookies from site: exp.2037

Site responded to privacy query

Site allows limited use of anonymizing services

Resume posting resulted in 0 spam from third parties

Resume posting resulted in 2 job leads

Note: You can browse the site using anonymizing tools, but you must apply for jobs through the site.

You can opt out of the Fastclick tracking cookie here:

http://www.fastclick.com/co_opt-out.html

CareerBuilder

www.careerbuilder.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits third party persistent cookies from:

2o7.net exp. 2008

Deposits persistent cookies from site exp. 2010

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in:

1 job offer from employer

6 third party solicitations to post at visit other sites from:

3 HotJobs/Yahoo

1 Accountemps

1 ijonn

1 Resumeblaster

(Resumes were posted openly).

Note: To opt out of the Omniture "2o7.net" tracking cookie, check here: <http://www.omniture.com/policy.html>. Scroll down to find opt out policy.

California Online Job Network

www.cajobs.com (Network of sites includes: www.sandiegojobs.com, jobsalaska.com, oaklandjobs.com, riversidejobs.com, sanjosejobs.com, losangelesjobs.com, orangecountyjobs.com, sacramentojobs.com, sanfranciscojobs.com.)

Privacy policy: Yes

No registration prior to looking at job ads

0 third party cookies of any type
Site did not respond to privacy query
Site allows variable use of anonymizing services
Resume posted resulted in 4 job leads
Resume posted resulted in 28 solicitations from various sites. Ex., resume2work,
ResumeBlaster. However, please see note below.
Note: Test Resumes posted to the California Online Job Network were cross-posted to at
least one other site (JobWareHouse.com) without researchers' prior knowledge.

California Teachers Net

California.teachers.net
Privacy policy: Yes
No registration prior to looking at job ads
0 third party cookies of any kind
Site responded to privacy query
Anonymizing services do not work well with this site
Resume posting resulted in 0 spam from third parties
Resume posting resulted in 5 job leads

CalJobs

www.caljobs.ca.gov
Privacy policy: Yes
Must register prior to looking at job ads
Must give SSN and date of birth to site before seeing jobs
0 third party cookies of any type
Site responded to privacy query
Site does not support use of anonymizing services
Resume posting resulted in 0 spam from third parties

CareerExplorer.net

www.careerexplorer.net
Privacy policy: Yes
No registration prior to looking at job ads
0 third party cookies of any type
Site did not respond to privacy query
Site allows use of anonymizing services
Search4College popup scripts
Resume posting resulted in 0 spam from third parties

CareerJournal

www.careerjournal.com
Privacy policy: Yes
No registration prior to looking at job ads
Deposits short term third party cookies from
 Doubleclick.net
Deposits persistent cookies from

WSJ.com 2013 (Site owner)

Deposits persistent cookies from careerjournal site exp. 2023

Site did not respond to privacy queries

Site allows variable use of anonymizing services

Resume posting resulted in 0 spam from third parties

Note: you may opt out of tracking from Doubleclick cookies here: <http://www.privacychoices.org/optout.htm>

CareerSite

www.careersite.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits third party persistent cookies from:

2o7.net exp. 2008

Site did not respond to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

Note: To opt out of the Omniture "2o7.net" tracking cookie, check here: <http://www.omniture.com/policy.html>. Scroll down to find opt out policy.

CollegeRecruiter.com

www.collegerecruiter.com

Privacy policy: Yes, but see note*

Must register prior to looking at job ads

Deposits short term third party cookies from:

Doubleclick.net

Deposits third party persistent cookies from:

Tribalfusion.com exp. 2038

Matchcraft.com exp. 2024

Site responded to privacy query

Site allows variable use of anonymizing services

Resume posting resulted in 1 spam from third parties for ResumeRabbit. Please note that researchers posted the resumes openly and opted in to receive marketing emails.

Note: You may opt out of Doubleclick cookies here: <http://www.privacychoices.org/optout.htm>

TribalFusion does not have an opt-out cookie. You may see its privacy policy here:

<http://www.tribalfusion.com/www/about/privacy.html>

College Central

www.collegecentral.com

Privacy policy: Yes

Must Register prior to looking at job ads (College system)

0 third party cookies of any kind

Site responded to privacy query

Site allows use of anonymizing services – N/A registration

Resume posting resulted in 0 spam from third parties

College Central is a network that your school must be signed up to use.

CollegeGradJobHunter

www.collegegrad.com

Privacy policy: Yes

No registration prior to looking at job ads

Deposited short-term third party cookies from:

Burstnet – session

Search4clicks.com – session

Doubleclick.net - session

Deposited persistent third party cookies from:

Qksrv.net exp: 2008

Advertising.com exp: 2008

Tribalfusion.com exp. 2038

Yahoo.com exp. 2010

Desposited persistent site cookies exp. 2010

Site responded to privacy query

Site allows use of anonymizing services

The job postings at this site click through to HotJobs.com. When you apply to HotJobs, the Yahoo.com privacy policy will apply. <http://privacy.yahoo.com/>

Note: you may opt-out of tracking by Doubleclick cookies here: <http://www.privacychoices.org/optout.htm>

You may opt out of Advertising.com tracking cookies here:

<http://www.advertising.com/OptOut.html> - data opt-out

<http://www.advertising.com/OptOut2.html> cookie opt-out

TribalFusion does not have an opt-out cookie. You may see its privacy policy here:

<http://www.tribalfusion.com/www/about/privacy.html>

CoolWorks

www.coolworks.com

Privacy policy: No

Registration prior to looking at job ads dependent on ad

Deposits third party persistent cookies If “Google search bar” used

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

Craigslist.org

www.craigslist.org

Privacy policy: Yes

No registration prior to looking at job ads

0 third party cookies of any type

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

Resume posting resulted in 2 job leads

Craigslist.org is a national community-oriented discussion site. Craigslist.org does not use any Web bugs or cookies at all, which is rare and a notably positive privacy feature at this site.

Edjoin/ CalTeach

www.edjoin.org

Privacy policy: Yes
No registration required prior to looking at job ads
0 third party cookies of any type
Site responded to privacy query
Site allows use of anonymizing services
Did not test post resume at this site
Note: Providing SSN at this site is strictly voluntary.

DICE

www.dice.com

Privacy policy: Yes
No registration prior to looking at job ads
Deposits short term third party cookies from:
 doubleclick.net
Site responded to privacy query
Site does not support use of anonymizing services
Resume posting resulted in 0 spam from third parties
You may opt-out of tracking by Doubleclick cookies here: <http://www.privacychoices.org/optout.htm>

DirectEmployers

www.directemployers.com

Privacy policy: Yes
No registration prior to looking at job ads
0 third party cookies of any type
Site responded to privacy query
Site allows variable use of anonymizing services
No resume database
DirectEmployers is a non-profit association of employers. Its site is a “pass through site;”
links here take you directly to the employer offering the job.

Execunet

www.execunet.com

Privacy policy: Yes
No registration required prior to looking at job ads: N/A
0 third party cookies of any kind
Deposits persistent cookies from site exp. 2033
Site responded to privacy query
Site does not support use of anonymizing services
Presence of www.deepmetrix.com on site
Profile posted at site resulted in 0 spam from third parties.
Please note that Execunet is a for-pay service.

FastWeb.com

www.fastweb.com

Privacy policy: Yes
Must register; may not see jobs in all circumstances
Deposits third party cookies from site owner:

Monster.com exp. 2013
0 third party persistent cookies
Site responded to privacy query
Site does not fully support use of anonymizing services
Must enable cookies or site will not function
FastWeb is a college scholarship search site. As with all sites, we recommend that you read the privacy policy before using the site.

FedJobs.com (Federal Research Service.)

www.fedjobs.com

Privacy policy: Yes

Must register prior to looking at job ads

Deposits third party session cookies from:

Axion-it.net

Linkexchange.com

0 third party persistent cookies

Short term cookies from site

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties.

FedWorld.gov

www.fedworld.gov

Privacy policy: Yes

No registration prior to looking at job ads

0 third party cookies of any kind

Site responded to privacy query

Site allows use of anonymizing services

No resume database

FlipDog

www.flipdog.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits persistent cookies from site owner

Cookie.monster.com (site owner) exp. 2013

Ads.monster.com exp. 2037

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

.

Hire Diversity

www.hirediversity.com

Privacy policy: Yes

No registration prior to looking at job ads
Deposits short term third party cookies from:
DoubleClick.net

Deposits third party persistent cookies from:
Bluestreak.com exp. 2013

Site responded to privacy query
Site allows variable use of anonymizing services
Resume posting resulted in 0 spam from third parties
Resume posting resulted in 1 job lead

Note: You can opt out of tracking by Doubleclick cookies here: <http://www.privacychoices.org/optout.htm>
You can opt out of Bluestreak tracking cookies here:
http://bluestreak.com/web/aboutus_privacypolicy.htm

HotJobs

www.hotjobs.com

Privacy policy: Yes
No registration required prior to looking at job ads
0 third party persistent cookies
Deposits persistent cookies from parent site:
Yahoo.com exp. 2010

Site responded to privacy query
Site allows use of anonymizing services
Resume posting resulted in 0 spam from third parties.
Resume posting resulted in 9 marketing emails (which researchers opted in to receive)
from parent company, Yahoo.com.

Note: to post your resume at HotJobs, you will be sent to a Yahoo! Registration page.
Yahoo! Is HotJobs parent company. While registering at Yahoo! you may choose to opt
in or out of marketing emails.

Idealist

www.idealist.org

Privacy policy: Yes
No registration prior to looking at job ads
0 third party cookies of any type
Site did not respond to privacy query N/A
Site allows use of anonymizing services
Profile posted resulted in 0 spam from third parties
This site does not allow resume posting, but you may upload a profile.

Ihire

www.ihireinc.com

Privacy policy: Yes
Must register prior to looking at job ads
0 third party cookies of any type
Site responded to privacy query

Site allows limited use of anonymizing services (registration required.)
Resume posting resulted in 1 site solicitation for ResumeBlaster
Resume posting resulted in 2 job leads
(Resume was posted openly).

IM Diversity

www.imdiversity.com

Privacy policy: Yes

No registration required prior to looking at job ads

0 third party cookies of any type

Site responded to privacy query

Site does not support use of anonymizing services (javascript issue)

Resume posting resulted in 0 spam from third parties

Job.com

www.job.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits third party session cookies from:

jobclicks.net

Deposits third party persistent cookies from:

advertising.com exp. 2008

Deposits persistent cookies from site exp. 2037

Site did not respond to privacy query

Site supports use of anonymizing services

Resume posting resulted in 0 spam from third parties

Note: You may opt out of Advertising.com tracking cookies here:

<http://www.advertising.com/OptOut.html> - data opt-out

<http://www.advertising.com/OptOut2.html> cookie opt-out

JobBankUSA

www.jobbankusa.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits third party persistent cookies from:

imrworldwide.com exp.2013

Site did not respond to privacy query

Site allows use of anonymizing services

Site allows full job application anonymously

Resume posting resulted in 0 spam from third parties

Note: You can find out more about IMRworldwide.com cookies at http://www.redsheriff.com/us/content/products_1_1.html.

Jobs.com

www.jobs.com

Privacy policy: No

No registration required prior to looking at job ads

Deposits persistent cookies from parent site Monster.com exp. 2037

Site did not respond to privacy query (no contact information for site)
Site allows use of anonymizing services
No resume test posted at this site
Note: Jobs.com is a “pass through site.” The links will eventually lead you to Monster.com.

JobWarehouse

www.jobwarehouse.com

Privacy policy available

No registration required prior to looking at job ads

Deposits third party session cookies from:

IAD.LIVERPERSON.NET EXP. NOV 2004

No privacy query submitted to site

Site allows use of anonymizing services

Result of Resume Posting: see below

Job Warehouse is a site that was not on the original study list. When researchers posted their resumes on SanDiegoJobs.com, the resumes were apparently cross-posted here.

LatPro

www.latpro.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits third party session cookies from:

Thruport.com

Deposits third party persistent cookies from:

Webtrends.live.com exp. 2020

Site responded to 2nd privacy query

Site does not support use of anonymizing services

Resume posting resulted in 0 spam from third parties

Legal Staff

www.legalstaff.com

Privacy policy: Yes

No registration prior to looking at job ads

0 third party cookies of any type deposited, however tribal fusion had “placeholders”

Site responded to privacy query

Site does not function well using anonymizing services

Resume posting resulted in 0 spam from third parties

Legal Staff is a site that complies well with many principles of Fair Information Practices. It has a good privacy policy, which although unconventional, is still protective of your overall data rights.

Medzilla

www.medzilla.com

Privacy policy: Yes

No registration required prior to looking at job ads
0 third party cookies of any type
Site responded to privacy query
Site allows use of anonymizing services
Resume posting resulted in 0 spam from third parties
Resume posting resulted in 2 job leads
The site specializes in medial, biotech, and pharmaceutical-related jobs. It has a detailed resume security and privacy policy and it has a record of strictly enforcing this policy on jobseekers' behalf.

Monster.com

www.monster.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits short term third party cookies from:

Doubleclick.net

Deposits third party persistent cookies from:

atdmt.com exp. 2008

in2.com exp. 2038 (Monster moving.)

Bluestreak exp. 2013

Deposits persistent cookies from site exp. 2037

Site responded to privacy query

Site allows variable use of anonymizing services

Resume posting resulted in 0 spam from third parties

Anonymizing services will work depending on whether or not a company has displayed full contact information in their job ad or not.

Note: You can opt out of Doubleclick cookies here: <http://www.privacychoices.org/optout.htm>

You can opt out of Atlas DMT tracking cookies here:

http://www.networkadvertising.org/optout_nonpii.asp

You can opt out of Bluestreak tracking cookies here:

http://bluestreak.com/web/aboutus_privacypolicy.htm

Monster Diversity

Diversity.monster.com

Privacy policy: Yes

No registration required prior to looking at job ads

Deposits third party persistent cookies from:

Bluestreak.com exp. 2013

Deposits persistent cookies from site: exp.2037

Site responded to privacy query

Site allows variable use of anonymizing services

Must have cookies enabled to effectively use the site.

Resume posting resulted in 0 spam from third parties

Anonymizing services will work depending on whether or not a company has displayed full contact information in their job ad or not.

Note: You can opt out of Bluestreak tracking cookies here:

http://bluestreak.com/web/aboutus_privacypolicy.htm

Monstertrak

www.monstertrak.com

Privacy policy: Yes

Registration prior to looking at job ads: N/A

Deposits persistent cookies from:

Monster.com 2037

Site responded to privacy query

Site does not support anonymizing services

Resume posting resulted in 0 spam from third parties

Site was displaying an invalid BBB privacy seal at the time site was researched

Note: Monstertrak is a site that may only be used by member colleges and universities, and by those who have accounts at those institutions. If you are attending a college or university, you will need to ask your career center about accessing this site. Monstertrak is owned by Monster.com.

Nacelink

www.nacelink.com

Privacy policy: Yes

No registration required prior to looking at job ads N/A

0 third party cookies of any kind

Site responded to privacy query

Site does not support anonymizing services

Resume posting resulted in 0 spam from third parties

Note: Nacelink is a site that may only be used by member colleges and universities, and by those who have accounts at those institutions. If you are attending a college or university, you will need to ask your career center about accessing this site. Nacelink is owned by the National Association of Colleges and Employers, a non-profit organization. NACE as an organization has a code of Principles for Professional Conduct that employers must abide by when working with college students. You can find the principles here:

<http://www.naceweb.org/about/princip.html>

NationJob.com

www.nationjob.com

Privacy policy: Yes

No registration required prior to looking at job ads

0 third party cookies of any type

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

This site has been established since 1988. It does not use cookies or Web bugs. It is notably privacy-friendly.

Net-Temps

www.net-temp.com

Privacy policy: Yes

No registration required prior to looking at job ads

0 third party cookies of any kind

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 3 solicitations from third parties
2 CareerXpress “visit our site”
1 hireusa.net “visit our site”
(Resume was posted openly.)

Resume.com

www.resume.com

Privacy policy: Yes
No registration prior to looking at job ads N/A
0 third party cookies of any kind
Site responded to privacy query
Site allows use of anonymizing services
Displaying invalid BBB Seal
No resume test posted at this site

Saludos

www.saludos.com

Privacy policy: No
No registration required prior to looking at job ads
0 third party cookies of any kind
Site responded to 2nd privacy query
Site allows use of anonymizing services
Resume posting resulted in 0 spam from third parties
Please note: must have 4-year degree to post your resume in the database.

Studentjobs.gov /USAJOBS

usajobs.opm.gov

www.studentjobs.gov
Privacy policy: Yes
No registration required prior to looking at job ads
Deposits session third party cookies from:
newjobs.com (Monster.com)
0 third party persistent cookies
Site responded to privacy query
Site allows variable use of anonymizing services
Must enable cookies or site functions poorly
Resume posting resulted in 0 spam from third parties
StudentJobs.gov and USAJOBS are the U.S. government’s official gateway job sites. The sites’ operations have been contracted out to Monster.com.

TrueCareers

www.truecareers.com

Privacy policy: Yes
No registration prior to looking at job ads
Deposits third party session cookies from:
Adjuggler.com

Thruport.com

0 third party persistent cookies

Site responded to privacy query

Site allows variable use of anonymizing services

Resume posting resulted in 0 spam from third parties

Note: TrueCareers is owned by a large financial company, Sallie Mae, which provides funds for educational loans, primarily federally guaranteed student loans originated under the Federal Family Education Loan Program (FFELP).

Vault

www.vault.com

Privacy policy: Yes

No registration prior to looking at job ads

Deposits short term third party cookies from:

Doubleclick.net

Deposits third party persistent cookies from:

valueclick.net 2028

realmedia.com 2010

Site did not respond to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

Resume posting resulted in 2 job leads

Note: To opt out of the Doubleclick cookie, check here: <http://www.privacychoices.org/optout.htm>

Note: To opt out of the ValueClick Opt tracking cookie, check here:

<http://www.valueclick.com/privacy.html>

Scroll to mid page and look for the link that says "Click here to go to Opt Out page."

Volt

Jobs.volt.com

Privacy policy: Yes

No registration prior to looking at job ads

0 third party cookies of any type

Deposits persistent cookies from site exp. 2037

Site responded to privacy query

Site allows use of anonymizing services

Verisign present on site.

Resume posting resulted in 0 spam from third parties

Site testing found that it is not feasible to use Volt without having cookies enabled.

WetFeet

www.wetfeet.com

Privacy policy: Yes

No registration required prior to looking at job ads

0 third party cookies of any type

Site responded to privacy query

Site allows use of anonymizing services

Resume posting resulted in 0 spam from third parties

WorkingWorld

www.workingworld.com

Privacy policy: NO

No registration required prior to seeing job ads

Site responded to privacy query

0 third party cookies of any kind

Site allows variable use of anonymizing services

Resume posting resulted in 0 spam from third parties

Workopolis

www.workopolis.com

Privacy policy: Yes

No registration required prior to looking at job ads

0 third party cookies of any kind

Deposits persistent cookies from site exp. 2010

Site responded to privacy query

Site does not support use of anonymizing services

Resume posting resulted in 0 spam from third parties

Note: Workopolis has a notably excellent privacy policy. When you post your information here, the default setting is that your resume will be made private.

XI. Consumer Tips for Job Searching Online

In any job search, it is important to circulate a resume. However, job seekers need to carefully minimize privacy issues related to resumes and personal data while still maintaining appropriate exposure to employers.

It is important for all job seekers to understand that employers, commercial job search sites, and resume databases vary widely in privacy practices and controls. Learning to choose a quality job search site and resume database with good privacy practices has become an important part of your job search if you plan to use the Internet as a job search tool.

Another key skill is to discriminate between valid job search related email and other offers and unhelpful maybe even fraudulent solicitations for your resume or personal data.

Remember, in the information economy, your resume and your personal information has a “street value.” It is important to protect your resume and personal information from people and businesses who want to use it primarily to make a profit instead of primarily to help you find employment. The World Privacy Forum and the Privacy Rights Clearinghouse have received credible complaints from consumers who had their identities stolen after using the services of online job search sites. Recently, an identity theft scam was operating through job fairs at State Departments of Labor and stole the

identities of hundreds of people who supplied resumes, SSNs, and financial information to a fraudulent company. You can go far in avoiding these kinds of problems by following these tips.

- Do not use a job search site, a resume writing service, a resume distribution service, or any job search service that does not have a posted privacy policy on its Web site. A privacy policy is a legal document that explains to you how a site or business will handle your personal data. It is also the basis of legal protection for you in case you run into any problems. If the privacy policy is not posted on the Web site, you do not have this legal protection. Posting privacy policies is voluntary. Most job sites at this point do post privacy policies. When you use the site, print out the policy and keep a copy of it for your records.
- No credible employer ever needs your bank account numbers, credit card numbers, mother's maiden name, or identifying characteristics such as eye color. If an employer requests these items from you, don't give them the information.
- If you plan on purchasing services from a commercial job site or writing service, look for a privacy policy that details how that service will handle your credit card data. Whenever possible, you may want to consider using PayPal to purchase services to protect your financial information from a company you do not know well.
- Some legitimate online job application sites and employment kiosks may sometimes ask for your Social Security Number and date of birth prior to posting a resume or applying for a job. (www.sportsauthority.com, www.albertsons.com, usajobs.opm.gov, studentjobs.gov, and many state job sites request this information.) Some of these sites conduct instant Social Security Number matching or background checks on your information to verify it. It is appropriate for you to allow a serious employer to use your SSN and date of birth to conduct a background check after you have engaged in the interview process.
- Not all sites that request your SSN and date of birth are legitimate. As a general rule of thumb, you should not supply this information up front, especially in combination with your credit card information. If you are unsure about a site's validity, please see the help section below for options.
- Cookies that are deposited on your computer from third party companies such as an advertising network (for example, Advertising.com or Doubleclick) may track your activities over many Web sites. Most sites will allow you to browse without accepting cookies. Set your browser to not accept any third party cookies. If you pick up any third party cookies, delete them. Or you may visit the opt-out pages of many advertisers and request that they stop tracking you with cookies.

- Research found that most sites allow you to look at job ads using anonymizing services. By all means take advantage of this. Using these services, which are free, will protect you from cookies and other privacy threats. www.Anonymizer.com, www.nonymouse.com, and www.junkbuster.com are sites to visit for more information about anonymous browsing. You can find a comprehensive list of these services at www.epic.org < <http://www.epic.org/privacy/tools.html> > .
- Even the most careful, conscientious sites cannot control your resume after an employer or a recruiter has downloaded it. Job sites do not have the ability to track or physically control how a recruiter or employer uses your resume after it is downloaded. Most sites watch for problems – such as rapid resume downloads – and enforce terms of use agreements with employers and recruiters. But let the job seeker beware. When it comes to resume databases, some responsibility does fall to the job seeker to understand the risks involved in posting a resume in a database.
- The more general the email job offer, the less valid it usually is. In the Biotechcareers.com emails to job seekers (a situation in which resumes were stolen), what stands out the most is that the emails asked jobseekers to send a resume to a new email address or to “update” their resumes. No *specific, credible job was offered at one specific, verifiable company*. Vague wording like “We have thousands of jobs” or “We work with major companies” is a red flag. Requests to send in a new copy of your resume can spell trouble, too. Avoid vaguely worded offers, and avoid sending your resume to general email resume solicitations after you have posted your resume online.
- Resume posting options for job seekers. Job seekers have several options to choose from in circulating a resume.
- One option is to reply to job ads directly without going through a third party. Look for a company-related email address to send your resume to.
- Another option is to post a resume directly on the Web site of the company you wish to work for.
- Working with one *carefully selected* “headhunter” or recruiter is also an option.
- Many job sites and resume databases let you mask your contact information or email address when you post a resume. This resume posting option allows you to control who contacts you or not. If you are going to post a resume online, this should be the only way you post it.

- Before posting a resume to any database, take the time to look for and read the privacy policy of that site and query the site owner with any privacy concerns . Be sure to look for specific privacy policy statements about resumes, registration information, and statements about how that information is used, stored, and shared. Pay particular attention to how long a site says it will keep or store your resume . Preferably, job and resume sites should state that they promise to keep your resume for a limited, specific amount of time, such as one to six months, after which the site will delete your resume. *Without specific, written statements about how long your resume may be kept, your resume can be archived for years, legally* . Most job seekers do not want resumes circulating after they have gotten a job.
- Before you post a resume, check to make sure you can delete your resume after you have posted it . Look in the job site's privacy policy for resume deletion instructions. If you don't find any such instructions on the site, write an email to the site and ask how or if you can delete your resume. If you are not satisfied with the reply, do not post your resume to that site. You must be able to delete your resume when you want to. After all, it belongs to you.
- If you plan on using a resume writing service in your job search efforts, get an agreement *in writing* that the service will not sell or share your resume or personal data with any third parties or partners . Also, ask to see the privacy policy of any resume writing services you may use and ask specifically about how the service handles and stores your resume. *This applies to traditional and online resume writing services.*
- Be aware that many resume writing services and job sites have affiliations with other businesses. When you are given recommendations, be sure to evaluate each recommendation on its own merit. Check for yourself if it is a good deal or not.
- Handling unsolicited email about your resume posting . If you post a resume to a resume database and receive unsolicited email other than from legitimate employers or recruiters, be sure to notify the site where you have your resume posted and tell them you have received the email. Be sure to forward the entire email you received to the site so that it can take action. Again, the more vague the email, the less legitimate it is likely to be.
- Keep good records . Be sure to keep a record of where you have posted your resume. Remember to go back and delete your resume from the sites where you have posted it after you have finished your job search.
- Post your resume sparingly. It is tempting to go to every job site you can find and

post your resume. Focus on quality, not quantity. If you believe you must post your resume online, hand-pick just a handful of sites that have good privacy policies and a good track record. Choose sites that other people working in your profession have had good luck with, and post only to sites that allow you to mask your contact information.

- Use a disposable email address. If you decide to post your resume to a site that does not allow you to mask your identity, then mask it yourself. Use an email address that you can cancel if you start getting spam, and don't give out your full name, phone number, or home address.
- Omit references on your resume . When you post a resume online with your references' names and phone numbers on it, you are giving their information away without their consent in what can be a very public forum.
- Your resume belongs to you. According to current copyright law, you own your resume and the copyright on it. If you don't like how your resume is being handled, you have the right to complain and take action.

Help for Job Seekers

If you believe your resume or personal job search data, including your email address or your name, has been shared or used in a way inconsistent with a job site's posted privacy policy, you have recourse through the Federal Trade Commission (FTC.)

You may file a consumer complaint with the FTC by calling (1-877-FTC-HELP) or by using the FTC's online filing system, located at <http://www.ftc.gov/> . Click on "File a Complaint Online."

If you have identity theft problems resulting from your resume posting, or if you are unsure about a company, visit the Web site of the World Privacy Forum and send in a complaint. Also, visit the Privacy Rights Clearinghouse www.privacyrights.org/identity.htm and the Identity Theft Resource Center www.idtheftcenter.org for facts and helpful information. The PRC provides other fact sheets relating to SSNs and financial information located at www.privacyrights.org/fs .

XII. Suggestions for Employers and Career Counselors

Employers are an important part of the data privacy solution. As the controller of job ads, employers have a great deal of say in how those ads are managed and displayed to applicants. For their part, college career counselors, as a critical part of the interface in a student's first professional job search, have a key educational role in the process.

Here are some recommendations.

- Employers, when you post a job ad, place detailed contact information in the job ad. This is how job seekers will be able to come to you directly. This contact information also allows job seekers to effectively use anonymizing services at job sites. If a site won't allow you to show detailed contact information, ask why, and push for allowing a direct application to you as the employer.
- Always ask if there are Web bugs, banner ads, third party cookies or other consumer tracking mechanisms on the pages where you post your job ads. Request that these mechanisms be removed so that you are the only one besides the job site that knows if a job seeker has looked at your ad. Checking pages for the presence of third parties is very simple; look in the HTML code of a page, and search for any servers other than yours or the company you are posting the ad on. A third party server will look like this in HTML code:

```

HREF="http://ads.adclicks.net/ads/banman.asp?ZoneID=33&Task=Click&Mode=HTML&SiteID=2&PageID=15689&RandomNumber=' +

```

- In this string above, **adclicks.net** is the third party code. To see this, look at the “view source” option in your Web browser.
- College career counselors, there is an excellent educational tool available to you right now. Carabella is a clever online game designed to appeal to and teach college age students about privacy choices. It was designed by a privacy expert and attorney, and it is an extremely useful (and fun) tool.
- Familiarize yourself with the OECD principles. These form the baseline of Fair Information Practices.
- Also, the OECD has an excellent privacy policy generator. If this is something you need, by all means access it and try it out. It is free, and is an excellent way of seeing where the bar is in terms of a full-bodied, robust privacy policy. It will help you see how consumer profiling technologies intersect with privacy concerns in a balanced way.
- The FTC has a series of key documents on consumer profiling. They will explain how ad networks work, how cookies and Web bugs work, and more. Xxx
- As you list your jobs at online sites, don't neglect your corporate home page. Make it simple for a job seeker to verify that a job is open, and who to contact to apply for that job. Be sure to disclose your practices, such as a corporate ASP that might be handling your jobs or any other outsourcing.

XIII. Credits

The World Privacy Forum conducted this research with funding assistance from the Rose Foundation Consumer Privacy Rights Fund. Without this assistance, this research would not have been possible.

- Pam Dixon, Principal investigator and author of study.
- Robert Gellman, Privacy and Information Policy Consultant.
- David Del Torto, CEO CryptoRights.
- Chris Hoofnagle, EPIC.
- Donald Harris, HR Privacy Solutions.
- Beth Givens, Director Privacy Rights Clearinghouse.
- Les Rosen, President Employment Screening Resources.
- Lance Cottrell, CEO Anonymizer.
- Richard M. Smith, Internet Privacy and Security Expert.
- Andrew Schulman, Software Litigation Consultant.
- Deborah Pierce, Privacy Activism.
- Kevin Davidson, Ogilvy.
- Stephen Keating, Former Executive Director, Privacy Foundation .

XIV. Methodology

A. Site Methodology

Site analysis involved over 1,000 hours of testing each site.

B. Methodology for Analyzing Resume Distribution Sites

- Sites were chosen based on a variety of factors including amount of brand exposure, overall site traffic, affiliation with major search site or known industry brand or individual, researchers personal knowledge of the sites, recommendations by industry members, and by the amount of e-mail solicitations for business received from the resume distributors after a resume was posted. High volume email solicitors made the list automatically.
- The principles of Fair Information Practices based on the 1980 OECD framework were used as the guide for privacy analysis.
- On October 16, 2003, the sites were visited for the final time and privacy policies, terms of use, and other relevant pages were captured and saved. The site policies were captured within one 12 hour period. These are the documents that were used for final analysis of the sites, in addition to any distribution results.
- Over the course of one year, researchers monitored resumes posted on all major job sites. All email promoting resume distribution services that was sent in response to those resumes was collected, tracked, and analyzed.
- Each site was analyzed for the following specific items:
 - Does the site have a privacy policy?

- Is the privacy policy posted conspicuously?
 - Does the privacy policy follow all of the FIPs?
 - Does the site have a terms of use policy?
 - Does the site encrypt or otherwise provide for secure credit card transactions?
 - Does the site display an online trust seal?
 - If yes, is the seal valid?
 - If yes to display question, and the seal is not valid, is the BBB or other seal program able to definitively confirm or deny the validity of the seal?
 - If yes to display question, does the site have a privacy policy?
 - Is the site a member of a BBB?
 - If yes, what is the site's rating, complaint number, and type, if applicable?
 - Does the site respond to privacy queries?
 - What is the response?
 - Does the site have an affiliate program?
 - If yes, what is the amount paid per referral?
 - If yes, has the affiliate program resulted in spam to jobseekers after the posting of a resume?
 - Does the site makes its full resume distribution list available to job seekers?
 - If yes, is the list accurate?
 - If not readily available prior to purchase, does the site respond to job seeker inquiries to view the list prior to paying for a resume distribution?
 - A sampling of resume distribution services were tested for results. Unique e-mail addresses were used for each resume, along with unique name aliases. All incoming e-mails and phone calls were recorded and sorted by email address and alias.
 - Researchers checked the Internet Web Archives for changes in privacy policies, old distribution lists, and other supporting information about the sites.
- Researchers conducted searches for legal actions regarding the sites.

C. Resume Writing Services Methodology

- Researchers chose the resume writing services based on their affiliation with a large or well-established job search site or career organization as well as the size or profile of the business.
- Also, industry professionals who were not resume writers were queried as to key businesses in the industry.
- After the services were selected, researchers called each service with information requests. The script researchers used on the phone was:

"We are a consulting firm which works with third-party recruiters and some of our clients have asked us to find additional resume sources. Does your company sell resumes or resume databases and, if you do, what is the cost."

- The researchers were instructed to tell the truth about where they worked if they were asked for that information. No resume service asked for the business name therefore none of them knew who was actually making the calls, although they had ample opportunity to know. Calls were placed by three researchers during the week of October 13 – 17.
- Each site was analyzed according to the Fair Information Practices framework as set out by the Internationally accepted OECD 1980 guidelines.
- Each privacy policy was downloaded and analyzed, when available.
- Sites were researched for consumer complaints, BBB online memberships, seal programs, and legal complaints.
- Researchers conducted general forensic data research on the selected sites to determine their technical practices.
- Researchers conducted informational research on the selected sites to determine general background information about the sites such as date founded, place of business, etc.
- One email query was sent regarding the privacy policy and practices of a site. The results were collected and tabulated.
- Prior to publication of this data, each resume writing service was notified 48 hours in advance of what the results were and were given a chance to respond to those results, correct errors, and discuss the results with the principal investigator on the study.
- Two resume writing services were removed from this study altogether after the research was complete.

Appendix A: Key Unicru Screens

APPENDIX A Unicru screens at Sports Authority

<<http://www.thesportsauthority.com/corp/index.jsp?page=jobs>>

<https://wss1a.unicru.com/hirepro/C149/locator.jsp>

We are including only the screens from the first screen through the end of the background check and EEO compliance screens. A longer range of screens which includes a portion of the personality test is available by looking at the Sports Authority application site online.

Each segmented area represents one screen.

(Begin Screens)

You have chosen the English version of the employment application with a Skills Assessment in English. Do you want to proceed? (The other choice is an English application with a Spanish Skills Assessment.)

If you want to proceed, press Next

If NO, Press `EXIT` to start again.

Thank you for applying for employment with The Sports Authority. We are a DRUG FREE Workplace. We've created an open, friendly place to work where honesty, mutual respect, teamwork and high standards are valued.

The Sports Authority depends on our Associates to provide our customers with a friendly, courteous and fun experience so they will visit again. If this is the environment you are interested in sharing with us, then please complete the following application.

The Sports Authority will provide reasonable accommodation to complete the application upon request consistent with applicable law. By proceeding, you are indicating that you have carefully read and understand the preceding statement and are not requesting an accommodation. If you are requesting an accommodation, please exit the application and notify store management..

This application process will take between 10 & 40 minutes depending on the position you are applying for. Your application will remain active for 120 days. The Sports Authority is an Equal Opportunity Employer.

Before beginning the employment application, we will ask for your Social Security Number, contact information and consent to perform a background check.

Social Security Number

IT IS VERY IMPORTANT that you enter the correct Social Security Number. If you are not sure of your correct SSN, please verify it with your SSN card. DO NOT guess at the number or enter incorrect numbers such as 000 or XXX. You must have a valid SSN in order for The Sports Authority to process your application.

Zip Code:

SSN (ex.: 123-45-6789): - -

Confirm SSN: - -

Thank you for your interest in working at The Sports Authority. As a part of the pre-employment process, we require that a background check be performed on all applicants. Before beginning the Employment Application, you will be required to consent to a background check. Furthermore, this authorization shall be valid for any subsequent job related inquiries made during my employment with The Sports Authority, should I become employed with The Sports Authority. If you do not wish to consent to a background check, please exit the system now by pressing EXIT. Otherwise, to continue, please press NEXT below.

The next few screens describe the types of checks which may be performed and ask for your authorization to release criminal history information reports, private companies' dishonesty, drug offense or violence reports, or credit bureau reports or motor vehicle reports as authorized under the Fair Credit Reporting Act ("FCRA").

The Sports Authority will make inquiries to Edge Information Management, Inc., a Consumer Reporting Agency, concerning your employment suitability and qualification.

You may contact Edge Information Management, Inc. at:

By Phone: 800-889-4473

By Mail: 1901 South Harbor City Blvd., Suite 401, Melbourne, FL 32901

or

Find contact information on Edge Information Management, Inc. using any computer connected with the World Wide Web at: www.edgeinformation.com

[Please do not contact Edge Information Management, Inc. for the status of your employment application. Edge Information Management, Inc. does not have access to this information and will not be able to respond to your request.]

By selecting option 1, I confirm that I know how to access the Edge Information Management, Inc. web site listed above.

I know how to access the web site

I do not know how to access the web site

I understand that I have the right to withdraw my electronic consent to this Authorization and the right to update information needed to contact me at any time by notifying The Sports Authority store manager or person in charge at this location.

If you decide at any point during this application to revoke your electronic consent, you must sign a paper Authorization form in order to continue with the application.

I understand that I may receive a paper copy of this consent (authorizing a background check) at no cost for 60 days by contacting Unicru at 1-800-338-6321 or visiting www.unicru.com for contact information.

[Please do not contact Unicru for results of the Background Check. Unicru does not have access to the report and will not be able to respond to your request.]

FCRA Disclosure and Authorization

I understand that for employment purposes The Sports Authority will verify all or part of the information I give The Sports Authority. I hereby authorize The Sports Authority to procure a consumer report and make any inquiry into my credit history, motor vehicle driving record, criminal and civil records, prior employment (including contacting prior employers), education as well as other public record information. I understand that inquiries may include any incidents of dishonesty, violence or drug related offences. This authorization shall apply to pre-employment inquiries only.

Consent to Authorization in Electronic Form

I understand that I have the right to receive this disclosure and background check authorization (the "Authorization") on paper and to consent in writing.

Please indicate your consent to receiving this Authorization in electronic form.

I Consent

I Do Not Consent

By entering the last 4 digits of your Social Security Number below you signify that you understand and agree to the terms outlined in the Authorization above. Otherwise, please exit the system now.

Are you applying for employment at a location in one of the following states?

California

Minnesota

Oklahoma

None of the Above

You have a right to obtain a free copy of any investigative consumer report obtained by The Sports Authority by selecting number "2" below. The report will be provided to you within three business days after the report is provided to The Sports Authority. The report will be sent to the address you listed above.

No, I do not wish to receive a mailed copy of the report.

Yes, I would like to receive a mailed copy of the report. ----

Under section 1786.22 of the California Civil Code, you may view the file maintained on you by the consumer reporting agency named above during normal business hours. You may also obtain a copy of this file upon submitting proper identification and paying the cost s of duplication services, by appearing at the Consumer Reporting Agency identified above in person or by mail. You may also receive a summary of the file by telephone. The agency is required to have personnel available to explain your file to you and the agency must explain to you any coded information appearing in your file. If you appear in person, a person of your choice may accompany you, provided that this person furnishes proper identification.

Thanks! Please proceed to the next screen to begin the employment application.

PERSONAL INFORMATION

< snip >

The following questions are completely voluntary. To comply with government regulations we must make a good faith effort to record this information on our applicants. Your answers will not be made available to anyone involved in the hiring process.

What is your race?

American Indian or Alaska Native

Asian

Black or African American

Hispanic or Latino

Native Hawaiian/ Other Pacific Islander

Caucasian or White

Sex:

Male

Female

Thank you.

Endnotes

¹ Please see Credits section for complete list of contributors.

² See “Hundreds Of Identities Stolen At N.J. Job Fair.” WNBC, Nov. 7, 2003. <<http://www.wnbc.com/news/2618945/detail.html>> Accessed Nov. 12, 2003. See also Associated Press, "Monster.com warns jobseekers of ID Theft," by Adam Geller, February 27, 2003.

³ See < <http://www.talentblast.com/> > .

⁴ See < <http://www.eliyon.com/PublicSite/public/default.asp> > .

⁵ See < <http://cs3-hq.oecd.org/scripts/pwv3/pwvhome.htm> >

⁶ See < http://www.epic.org/privacy/consumer/code_fair_info.html >.

⁷ See: < <http://usajobs.opm.gov> >. The SSN requirement can be found on the ResumeBuilder < <https://my.usajobs.opm.gov/userprofile.asp?resumeid=41595356&original=&builderid=37&viewresume=> > .

⁸ OPM News Release August 22, 2003. “ Over 3 Million visitors to USAJOBS and Over 50,000 Resumes Online.” < <http://www.opm.gov/pressrel/2003/CC-USAJOBS2.asp> > .

⁹ See in-store kiosks, or visit < <https://wss1a.unicru.com/hirepro/C149/locator.jsp> >

¹⁰ See Federal Trade Commission- Identity Theft Survey Report, September 2003. < <http://www.consumer.gov/idtheft/> >. Also see Written Testimony for U.S. Senate Judiciary Subcommittee

on Technology, Terrorism, and Government Information Senator Jon Kyl, Chairman, July 12, 2000. Testimony by:

Beth Givens, Director Privacy Rights Clearinghouse. <

http://www.privacyrights.org/ar/id_theft.htm>.

¹¹ See the EEOC fact sheet for more information < <http://www.eeoc.gov/facts/qanda.html> >.

¹² The basic email read:

“I had some trouble finding your privacy policy. Do you have one? Also, before I post my resume I want to be sure that it will not be shared with anyone but employers. I appreciate your reply and your help.”

¹³ For more information about cookies, please see CookieCentral < <http://www.cookiecentral.com/> > .

¹⁴ FTC Consumer Profiling Report to Congress See < <http://www.ftc.gov/opa/2000/07/onlineprofiling.htm> > and < <http://www.ftc.gov/os/2000/07/index.htm#27> >

¹⁵ For example, see <http://www.localcareers.com/privacy.htm>.

¹⁶ For example, Job.com has third party banner ads in its resume posting area from jobclicks.net.

¹⁷ Researchers received approximately a dozen emails soliciting inexpensive loans, credit cards, and other financial offers.

¹⁸ The RIAA vs. Verizon, case file can be found at EFF: < http://www.eff.org/Cases/RIAA_v_Verizon/>.

¹⁹ The NAI Principles are a self-regulatory scheme adopted by national advertisers. For more about this agreement, please see < <http://www.ftc.gov/os/2000/07/index.htm#27> > and < http://www.networkadvertising.org/aboutnai_nai.asp > .

²⁰ It is not possible to use a true anonymizing service when a site requires Javascripting to be operative. Most anonymizing services turn off Javascripting by default due to privacy and security issues relating to its use.

²¹ A proxy is a computer that stands between you and the machine you are accessing. Because of the use of an intermediary machine, you can keep your IP address and geographic location secret. For more on this see < www.junkbuster.com > .

²² SanDiegojobs.com privacy policy < <http://www.sandiegojobs.com/local/privacy.asp> > .

²³ ²³ *Medzilla, Inc. v Optimum Intelligence LLC, et al* Case No. CO2-2122R, U.S. District Court for the Western District of Washington at Seattle.

²⁴ A PDF copy of the invoice is available at <www.worldprivacyforum.org> . See “Resume Sale.”

²⁵ See “Hundreds Of Identities Stolen At N.J. Job Fair.” WNBC, Nov. 7, 2003. <<http://www.wnbc.com/news/2618945/detail.html>>

²⁶ See FastWeb’s privacy policy page at <<http://www.fastweb.com/fastweb/content/aboutus/privacy.ptml?SP=/sp/privacy> > . “If you give your permission to allow third parties to contact you, personal information about you (such as your contact information and other information collected during your visit to FastWeb) may be shared with colleges, universities, potential employers, recruiters/headhunters, data aggregators, marketers (possibly in the form of list rental), and other organizations. Regardless of your decision regarding the sharing of your personal information, we may share broad aggregate demographic data and related usage information with our business partners.”

²⁷ See <<http://www.eliyon.com/PublicSite/public/default.asp>> .

²⁸ See: <<http://networking5.eliyon.com/networking/> >

²⁹ See: <<http://directory.eliyon.com> > .

³⁰ See: <<http://www.esrcheck.com/articles/index.php>>.

³¹ <

http://www.resumeviper.com/emps_by_industry.php?Sid=2ac2bc573eda970b7625d259efa5eac5 > Check “Stats by Employer” to find this list from the ResumeViper home page.

³² <<http://www.paidresponse.com/> > Accessed October 17, 2003.

³³ <http://www.resumeviper.com/emplist_industry.php?industry=76 > ALYA, Inc. listed as of October 17, 2003. Also check BBB notation for ALYA, Inc. by contacting the The Louisville, KY Better Business Bureau.

³⁴ <<http://post.resumerabbit.com/go/view?page=privacy> >URL valid as of October 16, 2003.

³⁵ Researchers checked the source code to see if there was a technical error causing the problem. In the following code, you will see the “bbb_logo.gif” which is the name of the actual BBB logo picture. If the picture contained a hyperlink to the BBB, it would be included in this area of the code. This code was captured Oct. 16, 2003. The code did not contain a hyperlink to the BBB site.

© 2002 - 2003 Lee Hecht Harrison, LLC

All rights reserved</td>

<td align="center"></td>

<td align="center" valign="top">

³⁶ ResumeViper linked to a seal program search box from the BBB seal in its privacy policy.

According to a telephone interview with the BBB October 16, this linking is inappropriate when attached to an official BBB Seal. The link was :

<<http://www.bbbonline.org/consumer/SearchRel.asp?keyword=resumeviper&State=&ZipPostal=&program=4>> The link was accessed October 16, 2003.


³⁷ PR Newswire. “[ResumeRabbit.com](http://www.resumeviper.com) Partners with Industry Leaders to Maximize Benefits for Weary Job Seekers.” February 20, 2002.

³⁸ www.resumerabbit.com/ > “Affiliate link” Accessed October 19, 2002. The text of the affiliate pitch is as follows:

“Join the ResumeRabbit.com Affiliate Program
and earn \$20 bucks for each order! □

People are signing up for ResumeRabbit's One-Stop Resume Posting service like crazy! And our affiliate program gives you everything you need to instantly earn REAL CASH! You'll get:

- * Real-Time click-through & earnings reports,
- * Slick banners and text links to place on your site,
- * Monthly commission checks sent like clockwork,
- * Instant Program Activation - takes 3 minutes!

Since January 2001 ResumeRabbit.com has performed 100,000's of resume submissions for loads of happy customers. Other Publishers are cashing in on ResumeRabbit.com. Why shouldn't you? Turn your site into REAL CASH right now with ResumeRabbit.com!

³⁹ < http://www.resumeviper.com/affiliates_welcome.php?Sid= > Accessed October 19, 2003.

⁴⁰ < http://www.resumexposure.com/affiliate_info.asp > Accessed October 19, 2003.

⁴¹ < http://www.resumexposure.com/affiliate_info.asp > Accessed October 19, 2003.

⁴² <http://www.affiliatefirst.com/txt/Career/Resume/index.shtml> Accessed October 19, 2003.

⁴³ < <http://www.resumexposure.com/terms.asp> >

⁴⁴ See Resume Database Nightmare: Job Seeker Privacy at Risk. February, 19 2003. < <http://pamdixon.com/jobseekerprivacystudyfeb03.htm>>.

⁴⁵ See Resume Database Nightmare: Job Seeker Privacy at Risk. February, 19 2003. < <http://pamdixon.com/jobseekerprivacystudyfeb03.htm>>.

⁴⁶ See Resume Database Nightmare: Job Seeker Privacy at Risk. February, 19 2003. < <http://pamdixon.com/jobseekerprivacystudyfeb03.htm>>.

⁴⁷ < <http://www.resumewriters.com/termsfuse.html> > Accessed October 21, 2003.

⁴⁸ < <http://www.pathwinner.com/frame.asp?target=servicescareer> > See bottom of page, logos. Accessed October 21, 2003.

⁴⁹ Disclosure: The principal investigator on this project, Pam Dixon, has written a book for Peterson's, and has signed a book contract in the past with this company that resulted in payment.

⁵⁰ BBB Code of Online Business Practices, see Principle Three. < <https://www.bbbonline.org/reliability/code/code.asp> >.

⁵¹ See < <http://www.bbbonline.org/reliability/requirement.asp> > .

⁵² < <http://www.prwra.com/standards.html>> The PRWA standards state that members shall "Maintain strict confidentiality with every client, revealing information only upon written authorization by the client." This "upon written authorization" constitutes a loophole organizations have exploited terribly, with written client agreement taken as a single click on a terms of service agreement in fine print. The standards need to be updated and modified to close these privacy loopholes. The NRWA does not even go this far in addressing the privacy and confidentiality issue in its code of conduct. < <http://www.nrwa.com/Aboutus/Ethics.htm> >.

⁵³ The OECD privacy policy generator is available free of charge at < <http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm> > .

Updates to This Report

When we update this report or make any changes to it, we will make notice of it in this section.

November 12, 2003: One typo corrected, page numbers added, font size of endnotes increased. “Updates” section added to report and index.

November 11, 2003: Report issued on www.worldprivacyforum.org.