The World Privacy Forum

2003 Job Search Privacy Study

Job Searching in the Networked Environment: Consumer Privacy Benchmarks

November 11, 2003

Pam Dixon, Principal Investigator [i], Author

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. [ii]

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. [iii]

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. [iv] 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 garners 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 TitleVII 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 TitleVII.

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.

---

[i] Please see Credits section for complete list of contributors.
[ii] 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.
[iii] See < http://www.talentblast.com/> .
[iv] See < http://www.eliyon.com/PublicSite/public/default.asp> .