The Extent of Systematic Monitoring of Employee E-mail and Internet Use

Andrew Schulman
Chief Researcher
Workplace Surveillance Project
707-823-9179
707-477-3766 (cell)

July 9, 2001

Table of Contents

Introduction

Fourteen million employees -- just over one-third of the online workforce in the United States -- have their Internet or e-mail use under continuous surveillance at work. Worldwide, the number of employees under such surveillance is at 27 million, just over one-quarter of the global online workforce. The "online workforce" is those employees who have internet and/or e-mail access at work, and use it regularly.

Number of Workers under Continuous Online Surveillance

	Total Workforce	Online Workforce	Monitored Employees (Percent of Online Workforce)
United States	140 million	40 million	14 million (35 percent)
Worldwide	3 billion	100 million	27 million (27 percent)

Source: Privacy Foundation, 2001; Nielsen//NetRatings; U.S. Bureau of Labor Statistics; International Labour Organization

These measurements of the extent of workplace monitoring are derived from a study of self-reported user-base ("seats") and revenue figures of publicly-traded companies that sell e-mail and Internet monitoring software such as Websense and MIMEsweeper, and focuses on continuous, systematic surveillance.

Previous studies of the extent of workplace monitoring have been based on survey questions that were mailed to human resources managers, and have counted "spot checks" and other *ad hoc* examinations of employee activities to arrive at their figures for employee monitoring.

The Foundation¹s research suggests that *low cost of the technology,* more than any other factor, is driving the growth of e-mail and Internet surveillance in the workplace.

Surveillance vs. Spot Checks

Systematic monitoring raises a much larger privacy issue than spot checks. Monitoring all Internet activity and e-mail correspondence of all employees, rather than looking over the shoulder of just those employees of whom one has a reasonable suspicion, is essentially a dragnet-style "sweep," a blanket,*suspicionless* search that carries with it grave privacy concerns.

Several previous studies have looked into the difference between continuous surveillance and spot checks:

- A poll of corporate chief information officers in the U.S., conducted by *CIO* magazine, found that only 17 percent conduct sporadic employee e-mail checks, 16 percent never monitor employee e-mail, 11 percent check only on "problem employees," and 38 percent check only after there's been a complaint or productivity issue.
- In the UK, KPMG conducted a small survey in late 2000, and found that around 50 percent of the surveyed companies monitor Internet use "infrequently," around 20 percent monitor on a monthly basis, and only 11 percent monitor on a daily basis.

One reason for monitoring all employees without individual suspicion, is that, in a way, the entire workforce is now under suspicion. Organizations are increasingly concerned about the 'Internal threat"; there is a growing realization that most security breaches come from knowledgeable insiders rather than random outsiders. Network security then holds employees under the same suspicionless suspicion as random outside visitors to a website.

Our study's emphasis on continuous monitoring does not deny the importance of non-continuous monitoring. Many cases of employees fired or suspended for "inappropriate" Internet or e-mail use (see the Job Loss Monitor maintained on the Privacy Foundation's website) have not involved systematic monitoring.

For example, the South Dakota state government fired twenty employees in June 2001 for Internet misuse, not as a result of any systematic filtering or monitoring system in place to keep tabs on its 13,000 employees, but rather, according to Wired News, on the contents of one Web log report of the 100 users with the most hits over a three-week period.

However, 40 Xerox workers fired in 1999 for surfing forbidden websites were nabbed by software that recorded every website they had visited and every minute they had spent at those sites, according to the*New York Times*. In fact, Xerox routinely monitors the Web use of every one of its 92,000. Mike Gerdes, manager of information security at Xerox, has been quoted several times on the subject of employee monitoring, but declines to specify the products used.

The City of Boston's use of Elron Internet Manager is another example of the role played by systematic employee monitoring: The city uses Elron's software to monitor Internet and e-mail use on 4,000 computers spread out over 52 agencies. According to one report, officials have disciplined and even fired a handful of employees who violated the city's strict Web and e-mail policies on inappropriate material.

Many companies employ *ad hoc* monitoring, in that they've turned on logging in their proxy servers; at a later time, the company can examine the log files if the need or desire arises. It is also likely that some employers are systematically monitoring their employees, but without a product such as WebSense or MIMEsweeper, using instead standard Unix or Linux facilities such as syslog, or even with NT event logging.

Growing Business

Sales of employee-monitoring software are worth about $140 million a year, a return to the vendor of only a few dollars per covered employee: on average, only about $5.25 per monitored employee per year (and as little as $4 per employee, when the non-monitoring uses of these products, such as filtering for spam or viruses, are included).

Even figuring in reseller discounts and hardware costs, a large organization may end up paying less than $10 per year per monitored employee. For example, the U.S. Army recentlypurchased a 200,000-seat installation from

Websense; including hardware, the total cost was $1.8 million, or only about $9 per employee.

Over the past few years, employee monitoring has been increasing about twice as fast as the number of employees with Internet access. The online workforce in the U.S. as measured by Nielsen//NetRatings has grown by about 33 percent per year, to 40.7 million employees using the Internet in January 2001 from 30.6 million in January 2000.

In comparison, Websense reports that its software currently covers 8.25 million employees worldwide; two years ago, in July 1999, the figure was only 3.3 million. This represents a growth rate of about 60 percent per year. MIMEsweeper's currently reported 10 million users are up from 4 million as recently as November 1999; thus, sales of this e-mail-monitoring software have increased about 80 percent per year.

The purchasers of surveillance software include some of the top companies and government agencies in the country, according to the vendors' client lists:

Some major customers of employee-monitoring vendors*

MIMEsweeper American Fast Freight - article (10/15/99) Chicago Bridge & Iron - case study Zenith Electronics - case study
Websense American Express - article (3/28/00) Marriott - customer list, article (3/10/00) U.S. Army - press release (4/18/01)
SurfControl Barclays Bank Duracell - press release (4/4/01) U.S. National Park Service - article (2/5/01)
Elron Internet Manager City of Boston, MA - article (4/21/00) Texaco 20th Century Fox - case study
Tumbleweed MMS Skadden, Arps, Slate, Meagher & Flom LLP - press release (3/29/00) U.S. General Services Administration - client list

Source: Vendor disclosures; Privacy Foundation, 2001
*Some of these customers may not be using the employee-monitoring features of the products, and vendors may be listing an entire organization when in fact only one or more departments are using the product.

More than any other factor (even employer concerns over lost productivity or potential vicarious liability for employee activities), low cost may be what is driving the growth of monitoring e-mail and Internet activity. By contrast, activities that potentially pose as large a concern to employers, such as telephone use, are not yet monitored to this extent (except in call centers).

Monitoring Continues to Grow Despite Slowdown

The employee-monitoring business is facing the same slowdown as the rest of the computer industry, and lower IT spending could restrain the adoption of employee monitoring. Recently, problems have been reported for some companies involved in the employee-monitoring business:

- Tumbleweed laid off 20% of its staff
- N2H2 faces NASDAQ delisting
- Baltimore is seeing cutbacks in spending, and laid off 250 employees
- Telemate.Net was acquired by Verso, and is cutting 60% of its workforce
- Less dramatically, Websense's 1Q01 quarterly revenues increased only 17% over 4Q00, compared to a 23% increase from 3Q00 to 4Q00, and a 30% increase from 2Q00 to 3Q00.

However, Baltimore Technologies, which saw its quarterly revenues drop to $33 million in the first quarter of 2001

from $40 million in the fourth quarter of 2000, also picked up 445 new customers for MIMEsweeper during the same period.

General Methodology

This study looks at sales of monitoring products in the corporate and government markets. Some of the monitoring companies, such as N2H2 and SurfControl, also (or primarily) sell to schools, to monitor Web surfing by students. For the purposes of this study these educational sales were ignored, except to account for monitoring of teachers and staff.

There are at least four dozen companies that make employee-monitoring software, but a handful account for the vast majority of the business. The big publicly-traded companies include Websense, Baltimore Technologies, SurfControl, Elron Software, Telemate.Net, Tumbleweed Communications, N2H2, Secure Computing, and Symantec.

Employees Monitored Worldwide by Individual Software Products

Vendor/Product	Worldwide Monitored Seats
Baltimore MIMEsweeper (BALT; Dublin, Ireland)	7.25 million*
Websense (WBSN; San Diego CA)	5.75 million**
SurfControl SuperScout (LSE:SRF; Scotts Valley CA)	4.75 million
Symantec I-Gear, Mail-Gear (SYMC; Cupertino CA)	2.25 million
Elron Internet Manager (ELRN; Burlington MA)	1.9 million
Tumbleweed MMS (TMWD; Redwood City CA)	1.5 million
N2H2 (NTWO; Seattle WA)	1.5 million***
Telemate.Net (TMNT; Atlanta GA)	.45 million
Miscellaneous	1.65 million

Source: Privacy Foundation, 2001
*Baltimore Technologies self-reports 10.5 million; the Privacy Foundation estimates only 7.25 million used for monitoring.
**Websense self-reports 8.25 million; only 70 percent of customers install the Reporting module.
***N2H2 self-reports 16 million; 14.5 million are students.

For some of these companies, employee monitoring is only one of several lines of business, and some of the products used for employee monitoring can also be used for other functions. For example, monitoring employees' outgoing e-mail can be done as part of a larger e-mail system that checks all incoming mail for viruses or spam, monitoring employees' web accesses can be done as part of a firewall, or employee visits to specified websites can simply be blocked, without actually recording the attempted visit. Recording, rather than blocking, constitutes monitoring.

Some privately-held companies, such as SRA, specialize in higher-priced products for the financial industry. SEC and NASD regulations, covering several hundred thousand employees, require monitoring of broker-dealer communications with the public, including e-mail. They were included in the study under Miscellaneous.

A variety of figures were used to determine the number of employees monitored by each product. Some vendors, such as Websense and Baltimore Technologies, maker of MIMEsweeper, publish their own estimates of how many people worldwide use their software. Revenue figures of other vendors, supplied in their annual and quarterly SEC filings, were divided by an estimate for the annual revenue generated per monitored employee. When a product could also be used for non-monitoring purposes, the number of monitored employees was correspondingly reduced. The industry's annual growth rate was used to bring older figures up to date. (See Note on Extrapolated Figures below.)

The increasing use of HTML as an e-mail format, and the popularity of web-based e-mail sites such as Yahoo! and Hotmail, make the distinction between Internet and e-mail monitoring a little fuzzy. However, the study found that monitoring of Internet use (primarily Web surfing, but also including other Internet protocols such as IRC chat, news, ftp, and telnet) is more prevalent than monitoring of e-mail. Websense is the most frequently used Internet-monitoring product, and MIMEsweeper is the most frequently used e-mail-monitoring product.

Internet vs. E-mail Monitoring*

	Online Workforce	E-mail Monitoring	Internet Monitoring
United States	40 million	6.25 million (15 percent)	7.75 million (19 percent)
Worldwide	100 million	12 million (12 percent)	15 million (15 percent)

Source: Privacy Foundation, 2001
*Doesn't account for employees whose Internet and e-mail are both monitored.

The current study does not account for those employees whose Internet and e-mail are *both* monitored. This overlap could occur if, for example, the employer has installed both the I-Gear and Mail-Gear products from Symantec, or is using Websense together with MIMEsweeper. This would *reduce* the total number of monitored employees.

How much the number would be reduced is difficult to estimate. However, taking the Symantec example, in 1999 when user figures were last available, there were 4 million users of I-Gear, and 1 million users of Mail-Gear. The maximum possible overlap would be 1 out of 5 million, or 20 percent. Since then, e-mail monitoring has become more important, as indicated by MIMEsweeper's larger user base than that of Websense, so the maximum possible overlap could be 25 percent. If we arbitrarily decided that half of the possible overlap is actual overlap, then the number of online workers under constant online surveillance worldwide would be closer to 20.25 million and 10.5 million in the U.S., or 20 percent of the global online workforce and 26 percent of the U.S. online workforce.

However, our existing 27 million and 14 million estimates are in fact quite conservative underestimates, because we have had to skip over one possibly major product, Raytheon SilentRunner, and have omitted employee monitoring that is performed without using one of the commercially available products. The IT departments at some large companies could be taking a do-it-yourself approach to employee monitoring, as mentioned above.

In addition, this study does not take into account products that have employee monitoring as a secondary feature. For example, the Webtrends Firewall Suite includes the SurfWatch monitoring product. According to a WebTrends FAQ, their firewall "reports on all employee Internet activity as read by firewall or proxy servers and highlights any visited sites with content pertaining to sexually explicit, violence, hate speech, gambling, and drugs/alcohol. Optional productivity-related categories include sports, fashion, entertainment, games, and shopping." (WebTrends was recently bought by NetIQ, for about $1 billion in stock.)

The Online Workforce

The number of employees whose internet and/or e-mail is monitored should be compared, not with the total number of employees in the U.S. or worldwide workforce, but with the number of employees who actually have Internet and/or e-mail access at work, and use it regularly.

This study uses a figure of 40 million for the U.S. online workforce, the number of employees who actually have Internet and/or e-mail access at work, and use it regularly. In May 2001, Nielsen//NetRatings reported the total at-work "Internet universe" in the U.S. at 42.2 million employees; the "active" population was 34.5 million employees, without accounting for e-mail.

The total U.S. workforce is currently around 140 million workers, according to the Bureau of Labor Statistics. Thus, about 30 percent of the U.S. workforce can be considered online.

Worldwide, Nielsen//NetRatings reported in June 2001 that 429 million people have Internet access. How many of these are at work? In the U.S., the ratio of the at-home to the at-work Internet population is 4 to 1. Using the 4-to-1 home-to-work ratio globally yields a worldwide online workforce of a 107 million. However, according to Nielsen's report, "in both Europe and Asia Pacific, home access is a more common source of Internet access than work based access.... Even for those who do have Internet access at work, home is more likely to be the location of use of the Internet." Therefore, this study assumes a global online workforce of 100 million out of the 3 billion workforce reported in the International Labour Organization's World Employment Report, 2001.

Most of the revenue figures used in this study include sales in Canada as well as the United States. Nielsen//NetRatings says the at-home Internet population in Canada is 14.5 million. In the US, the ratio of the at-home to the at-work internet population is 4:1. If the same ratio applies to Canada, this would yield a figure of 3.6 million. For this study, we will take 4 million as the size of the Canadian online workforce. This brings the total

size of the North American online workforce to 44 million. Note that the U.S. online workforce represents 90 percent of the North American online workforce. The study relies on this when turning vendor North American revenue figures into U.S. revenue figures.

Comparison with Previous Studies

How do the new Privacy Foundation figures compare with previously available figures? The most widely cited study, the annual American Management Association (AMA) survey of "Workplace Monitoring & Surveillance," found in 2001 that "More than three-quarters of major U.S. firms (77.7 percent) record and review employee communications and activities on the job, including their phone calls, e-mail, Internet connections, and computer files."

The Privacy Foundation's results are not necessarily inconsistent with the AMA figures themselves, but with the way the AMA figures are conventionally interpreted:

- A careful reading of the AMA results shows that "Most respondent firms carry on surveillance practices on an occasional basis in the manner of spot checks rather than constantly or on a regular routine." Spot checks can include anything from looking through log files on the company server to reviewing computer use as part of an ongoing investigation into a particular employee's problem behavior. In effect, the AMA asked HR managers, "Has your organization ever had occasion to monitor employees?" In contrast, the Privacy Foundation study focuses on "surveillance" as continuous and systematic monitoring.
- The AMA's 77.7 percent figure includes recording and reviewing telephone conversations and voice mail messages, storage and review of computer files, and video recording of employee job performance, as well as storage and review of e-mail messages and monitoring of Internet connections. The Privacy Foundation study looks exclusively at continuous monitoring of Internet use and e-mail. Other technologies such as keystroke logging and other forms of personal-computer monitoring, video surveillance, telephone or voice-mail monitoring, and location tracking, were not examined.
- The AMA figure for e-mail monitoring exclusively is 46.5 percent of major U.S. firms (up from 14.9 percent in 1997); its figure for monitoring Internet connections is 62.8 percent of major U.S. firms (up from 54.1 percent in 2000, the first year the AMA asked HR managers about this practice). In comparison, the Privacy Foundation found 15 percent of the U.S. online workforce under e-mail monitoring, and 19 percent under Internet monitoring. Both studies found that Internet monitoring is more prevalent than e-mail monitoring.
- The AMA notes that its sample "accurately mirrors AMA's corporate membership and client base, who together employ one-fourth of the U.S. workforce ... the sample does not accurately reflect policies in the U.S. economy as a whole, where smaller firms predominate." The Privacy Foundation is looking at the number of employees monitored; the AMA is counting the number of major firms that at some point have engaged in monitoring.
- Because it is based on worldwide revenue figures, the Privacy Foundation study also measured non-U.S. monitoring.
- Revenue figures also indicate how inexpensive monitoring is, and how dependent monitoring is on IT spending.
- Perhaps most importantly, the AMA survey asked HR managers to respond to a questionnaire. The Privacy Foundation's use of industry revenue figures provides a more objective measurement of the extent of monitoring.

Another widely cited study, conducted by International Data Corp. (IDC) on behalf of Websense, maintains that what Websense calls the "Employee Internet Management" (EIM) business should grow at an annual growth rate of 55 percent.

This is clearly inconsistent with any notion that three-quarters of employers *already* engage in this type of employee surveillance. However, it does correlate with the Privacy Foundation results, the only caveats being that employee monitoring is affected by larger fluctuations in IT spending, and that EIM obviously cannot grow indefinitely -- at least not without merging with some other function, such as internal firewalls, or taking on additional responsibilities, such as monitoring of telephone conversations and voice mail.

Vendor Response

Some of the vendors expressed concern that their revenue figures should not be related in any direct way with the size of their user base, and/or that their revenue model (involving deferred revenues, for example) was too

complex to handle in this way. Others pointed out that what we call "employee monitoring" could not be so easily split off from other functions of their product, such as security (virus detection, network firewall, etc.).

Conclusion

The systematic monitoring of Internet and e-mail communications in the workplace is a relatively new phenomenon, with reverberations yet to come in labor law and human resources, as well as employee behavior and morale.

Monitoring an entire workplace in order to catch slackers, deter inappropriate Web surfing, or perhaps to ferret out criminal behavior, may strike some employers as judicious. But it may also inject an air of suspicion and hostility into the workplace. Furthermore, the monitoring of an entire workplace to protect the organization from liability for "hostile environment" lawsuits may be creating its own peril for employers. By tracking and storing a detailed audit trail of employee activities, organizations may by inadvertently stockpiling large amounts of potential evidence that could be used against them in future litigation. This is particularly significant in government offices, where logs and reports produced by employee monitoring may be considered public records and accessible under Freedom of Information Act requests.

A key question implied, but not addressed, by this research report is whether employers are giving employees sufficient notice of continuous Internet and e-mail monitoring. Because companies can use (or be seen as using) employee-monitoring logs as a kind of "wishing well" to justify actions against employees, including dismissals and layoffs, employers would be well advised to disclose to employees what is being monitored and why. Employees, meanwhile, should make it their business to learn which monitoring systems are in place, and what the capabilities are.

While employers may fear that putting such knowledge in the hands of employees may allow employees to circumvent these systems, the practice of keeping employees uninformed about the details of monitoring may be tantamount to entrapment. Telling employees exactly what monitoring system is in place, and letting them see what the system's capabilities are, is likely to have more of a deterrent effect than a vague reference by an employer who "may monitor your activities for enforcement purposes."

Notice of monitoring in the form of a boilerplate paragraph in the employee handbook is inadequate. A "splashscreen" warning each time an employee starts the computer is an absolute minimum for adequate notice of ongoing continuous monitoring of online activities.

Notice, however detailed, may not be enough. As with the debates regarding information kept on private citizens in commercial and government databanks, there should also be access. Employees should be able to see, review and append comments to the logs and reports that have been kept by employers on their e-mail and Internet activities.

One of the main lessons from this study is that today, more than any other factor, inexpensive technology is driving the growth of employee monitoring. It's cheap and easy to record and store more and more office activities that once were ephemeral. Shoshana Zuboff's fascinating early look at employee monitoring, *In the Age of the Smart Machine: The Future of Work and Power* (Basic Books, 1988) refers to this as the "textualization of work," which means that increasingly, employees' activities end up being recorded in files.

An important area for future study will be whether technological "convergence," such as Internet telephony and digital video, fosters the same type of widespread monitoring of phone conversations, voice mail and visible activities that is apparent today for Internet and e-mail use.

APPENDICES

Appendix A: Notes on Extrapolated Figures

In the course of examining revenue numbers of employee-monitoring companies, we found several figures that we then sometimes used to supply missing information for other companies:

- As noted earlier, some products used for employee monitoring also have non-monitoring uses such as virus checking and spam elimination. The major assumption in this study is that only 70 percent of such use should really be counted as employee monitoring. This figure was supplied by Websense, as an estimate of the percentage of their customers who turn on Websense's optional reporting feature.
- Some companies didn't break out U.S. or North American sales. When necessary, this study assumed that 60 percent of total sales come from North America. This is extrapolated from available figures. For example, Websense reports in its Q1 2001 report that "we derived 34 percent of revenues from international sales." SurfControl's statement for the 9 months ended Feb. 28, 2001 shows North American turnover as 78 percent of the total. On the other hand, Baltimore Technologies (based in Ireland) derives only 22 percent of revenues from sales in the Americas; however, Content Technologies, from which Baltimore acquired the MIMEsweeper product line, had at the time of the acquisition (Sept. 2000) 42 percent of its sales in North America. North American sales (U.S. and Canada) account for just under 60 percent of the revenues of the firms that produce these products.
- In some cases, we had older figures that we needed to bring up to the present. As noted earlier, IDC figures the industry's growth rate at 55 percent per year. While this is not sustainable, it does not exaggerate reflect industry trends until recently, and may even underestimate them. As noted earlier, the user base reported by Websense and MIMEsweeper has increased 60 percent and 80 percent per year, respectively.
- Over the years, some of the companies in this study have published both revenue figures and the number of "seats" or "users" of their software. Since these products are frequently sold on an annual subscription basis, dividing annual revenues by users provides a rough sense of how much an employee-monitoring company makes per monitored employee each year.

  For example, Websense announced Q1 2001 revenues of $6.7 million, representing more than 8.25 million worldwide customer seats, pre-sold on a subscription basis. If the Q1 figures are stretched out to an entire year, this means $26.8 million, or only about $3.25 per customer seat. Content Technologies, at the time of its acquisition by Baltimore, claimed 6 million users and annual revenues of about $25 million, or about $4.15 per employee.
  A small Australian company, EmuTech, before its acquisition by SurfControl, had annual revenues of $242,000 and covered 45,000 users; this comes out to $5.35 per user.
  These companies (with the exception of a few that are targeting the financial market, in which SEC and NASD regulations require e-mail monitoring) don't make much per user. About $4 a head seems to be the industry standard. However, as noted above, not all the "users" of these products can really be considered as under surveillance. By taking the 70 percent monitoring figure noted above, and using the Websense and old Content Technology figures, we came up with a rough figure of $5.25 per *monitored* employee:

  ```
  WBSN $6.8 million * 4 = $27.2M + old Cont. Tech. $25 million = $52.2 million
  WBSN 8.25 million employees + old Cont. Tech. 6 million employees = 14.25 million employees * .70
  = 9.95 million employees
  $52.2 million / 9.95 million employees = $5.25 per monitored employee per year
  ```

- Some companies selling monitoring software to both the corporate/government and educational/home markets do not provide separate revenue figures. This study is concerned only with employee monitoring. SurfControl's financial statement for the 9 months ended Feb. 28, 2001 showed education/home sales accounting for 14 percent of revenues. Symantec reported that "almost half" its sales are corporate. A Frost & Sullivan study found that the "content filtering" business (which has a large overlap with employee monitoring) generated $119 million in revenue in 2000, of which corporate customers accounted for 77 percent and education 16 percent. Unfortunately, there is too wide a range here to derive a sensible average corporate/government-sales percentage. In addition, enterprise sales are likely more lucrative than educational sales (precisely why many "censorware" companies entered the enterprise market in the first place), so that $1 of educational revenues covers more students than $1 of enterprise revenues covers employees.
- It's sometimes useful to know roughly how many employees there are at the average customer site. Websense currently reports 8.25 million seats and 13,000 customers, or about 635 seats per customer. MIMEsweeper reports 10.5 million seats and various reports 8,000 and 10,000 customers, or between 1,050 and 1,300 seats per customer. SRA Assentor reports over 100,000 seats at over 75 firms, or about 1,300 seats per firm. It is reasonable to say that a typical customer has about 1,000 seats.

Appendix B: Internet Monitoring

Totals for Internet Monitoring, Worldwide

Websense	5.75 million
SurfControl Web Filter	3.75 million
Symantec I-Gear	1.8 million
N2H2	1.5 million
Elron IM Web Inspector	.95 million
Telemate.Net	.45 million
Misc.	1.2 million
Total	15.4 million

"Internet monitoring" refers primarily to examination and logging of an employee's Web surfing. Most of the products look at the URLs rather than the page contents. Some have the option to log only the domain name (e.g., "playboy.com") rather than the full URL (e.g., "http://www.playboy.com/2001/april/playmate.gif").

"Secure" web pages are a major hole in most products' monitoring. URLs that start with "https://" are frequently invisible to these products, or only the domain name is visible. Some of the smaller companies make products that install, not on a network server, but right on the PC used by the employee. These products, such as WinWhatWhere Investigator, *can* see all https:// requests. While such products make up a tiny fraction of the market (see below), there does appear to be a small trend toward locating a client "agent" on the employee's PC; this agent could be used to monitor https:// traffic.

Apart from web surfing, these Internet monitoring products can also frequently see traffic related to other Internet protocols, such as ftp, telnet, news, and IRC (chat). Some of these products don't watch AOL Instant Messenger (AIM), RealPlayer, Napster-like file-sharing services and so on, but they do block access to the sites from which an employee would download these tools.

Websense	WBSN; San Diego CA; http://www.websense.com
Product	Websense Enterprise Websense partners with MIMESweeper for e-mail.
Revenues	Q1 2001: $6.8 million Q4 2000: $5.8 million Q3 2000: $4.7 million Q2 2000: $3.6 million Q1 2000: $3.1 million
Price	Websense has an "ROI [return on investment] Calculator" at its website, which uses a figure of $15 per employee, per year. The U.S. Army recently purchased a 200,000 "seat" installation from Websense; including cache engines and Ethernet switches, the total cost was $1.8 million, or only about $9 per employee. Websense "channel partners" get a 30% discount.
Seats	More than 8.25 million worldwide customer "seats," pre-paid on a subscription basis. Websense is "used by more than 13,000 organizations worldwide, including 244 of the Fortune 500." The top five users of Websense Enterprise based on subscription fees since January 1999, include American Express, AT&T Wireless Services, Compaq Computer and IBM. As recently as July 2000 Websense claimed only 5.4 million users, and for July 1999, only 3.3 million.
Monitoring	Websense can "enforce policies by employee username or group membership. This enables reporting based on username, which is easier to interpret than IP addresses. Companies often need to create particular access policies for different employees and departments, based on job requirements or security level" (Buyer's Guide). In its default configuration, Websense merely *blocks* certain websites, and does not keep any record of attempts to visit these sites, much less of successful visits to non-blocked sites. It is the recording, rather than the blocking, that constitutes monitoring or surveillance. Websense has a separate module, Websense Reporter, which records all web accesses (not only attempted accesses blocked by Websense, but also all non-prohibited web surfing) -- and, significantly, 70% of Websense's customers choose to install this Reporter module, according to a company public-relations spokesperson.
North America	In Q1 2001, 34% of revenues from international sales, compared to 29% for Q1 2000

Corporate	WebSense is targeted entirely at the corporate and government markets.
Growth	User base has grown about 60% per year. Websense's Q1 2001 quarterly revenues increased 17% over 4Q 2000, compared to a 23% increase from 3Q 2000 to 4Q 2000, and a 30% increase from 2Q 2000 to 3Q 2000.
Monitored Employees	8.25 million * 70% = **5.75 million** (This assumes that the 70% using Websense Reporter are evenly distributed among company sizes. It seems likely to be used more by larger companies, in which case 5.75 million is too low.)

SurfControl	London: SRF; Scotts Valley CA; http://www.surfcontrol.com
Product	SuperScout Web Filter. Also has SuperScout E-mail Filter (see below).
Revenues	Corporate turnover for filtering product: 9 months ended Feb. 28, 2001: $24.7 million 9 months ended Feb. 28, 2000: $ 4.8 million
Price	SurfControl has an ROI Calculator at its site that uses a sliding scale, from $1195 for 50 or fewer employees, to $45,000 for 10,000 employees, but with an average of $10 per employee. Average order is $4,500.
Seats	"SurfControl now has over 35,000 corporate customers including 19 of the FTSE 100 and over 100 of the Fortune 500. In addition, SurfControl has over 18,000 installations in educational establishments around the world and 9.2m users of its home product - CyberPatrol" (Press release). Websense claims that SurfControl has less than 2 million corporate seats.
Monitoring	SurfControl has some issues associating individual usernames with web-surfing logs. "Enterprise User monitoring utility... will allow SurfControl to resolve usernames of clients located outside the local domain."
North America	SurfControl's financial statement for the 9 months ended Feb. 28, 2001 shows North American turnover as 78% of the total.
Corporate	Financial statement for the 9 months ended Feb. 28, 2001 showed education/home sales accounting for 14% of revenues.
Growth	About 25% per year: Q4 2001 filtering turnover was $10.5 million; Q4 2000 filtering turnover was $8.4 million.
Comments	SurfControl says in its 2000 annual report that the Corporate Internet Access Control (CIAC) market has less than 1% penetration.
Monitored Employees	Taking the claimed 35,000 corporate customers, and multiplying by the $4,500 average order, would yield accumulated revenues of $157 million, far in excess of SurfControl's reported revenues. Dividing by the average price of $10 per seat, would yield an amazing 15.7 million corporate seats -- a number SurfControl would surely emphasize over its 9.2 million home users. It is more sensible to start with SurfControl's current annual filtering revenues of about $30 million, take 85% of this for corporate and government sales, and divide the resulting $25 million by our estimated $5.25 per monitored employee, yielding 4.75 million monitored employees worldwide. However, account must be taken of SurfControl's e-mail filtering product, treated separately below. Figuring 1 million for SuperScout E-mail Filter (using a rough 3:1 ratio derived from Symantec figures) leaves **3.75 million** employees whose non-e-mail Internet activity is monitored with SurfControl.

Elron Internet Manager	Subsidiary of ELRN; Burlington MA; http://www.elronsw.com
Product	Web Inspector (Message Inspector is treated separately below). Elron purchased this from ON Technology (where it was known as ON Guard Internet Manager) in Feb. 1998; ON had previously purchased it from Purview.
Revenues	Elron Software is a privately-held subsidiary of ELRN, but ELRN's "Manager's Report" for Q1 2001 does include separate revenue figures for Elron Software: Q1 2001: $2.2 million Q1 2000: $2.8 million "The decrease was primarily due to the change in sales mix as Elron Software reduced emphasis on marketing

	of its legacy products, resulting in a decrease of approximately $0.4 million in net revenues from these products." Annual revenues for Elron's "Internet Policy Management" products, then, are about $10 million.
Price	Elron's prices range from $6.30 per government user in installations of 25,000 and more users, to $35 per corporate user in installations of 25 or fewer users. Reseller discounts are 15% for associates and 30% for "diamond partners." For an office of 100-249 corporate users of either Message Inspector or Web Inspector, list price is $25 per use; for an office of 1000-1,249, it's $13. It's not a subscription-based product, but does have maintenance agreements at 20% of list price.
Seats	An Elron press release from December 1999 refers to "an installed base of six million licensed users at over 13,000 organizations" for Elron Software's Internet Products Division. Curiously, however, starting some time in 2000, Elron press releases started saying that "Elron Software has licensed its products to over 3,500 organizations and government entities," and doesn't mention the number of licensed users. Asked about how 13,000 organizations in late 1999 became only 3,500 in 2000, a marketing spokesperson for Elron Software noted that "in the 2000 and forward releases, we are focusing solely on customers that are using our Internet Manager Policy Management products (Message Inspector, Web Inspector, Anti-Virus and Firewall). Previous numbers included customers using our sunsetted SofTrack product and other legacy products. SofTrack was a software application used to track which applications are actually installed on a desktop computer, and thus does not fall under the Internet Policy Management umbrella." Websense claims less than 1 million seats for Elron Internet Manager.
Monitoring	Elron IM "provides accurate user accountability enabling reporting of Web usage activity by user, regardless of the IP address or workstation used to access the Web -- even in environments with roaming users or with addresses assigned dynamically via DHCP" (Press release). We should discount for the Anti-virus and firewall products, which are aimed at the external rather than the internal threat, and thus not part of the employee-monitoring market.
Corporate	The product appears to be aimed squarely at the corporate market.
Monitored Employees	Clearly, the 6 million figure from late 1999 can't be used. We could take the reduction from 13,000 organizations to 3,500, figure that the average size of the organization hasn't changed, apply this to the 6 million, and end up with a figure of about 1.5 million. This sounds like pure guess work, but if we figure $10 million in revenues, and divide by $5.25 per monitored employee (this figure discounts non-monitoring use), we come up with a number in the same ballpark: about 1.9 million monitored employees. We need to subtract an estimate for Elron's e-mail monitoring product, however. Using the 3:1 ratio derived from old URLabs figures (see above), we get would get 1.4 million for the web monitoring product. However, from looking at Elron's product offerings, it seems more evenly divided, so just give **.95 million** to each product.

N2H2	NTWO; Seattle WA; http://www.n2h2.com
Revenues	Total revenues for Q1 2001 were only $1.89 million. For the 6 months ending March 31, 2001, they were $4.375 million, down from $5.182 million in the same period a year earlier. The decrease represents N2H2's movement from an advertising model to subscriptions. Obviously, industry standard revenues per monitored worker can't be applied to N2H2.
Seats	The company boasts "a customer base of more than 16 million enterprise, educational and home consumer users." N2H2 has recently announced that it covers 14.5 million students So with the total figure of 16 million, we now know that N2H2 covers, at most, 1.5 million employees. It seems possible that many of these 1.5 million employees are teachers and staff at schools. According to the National Center for Education Statistics, the U.S. national average student/teacher ratio is 16.2/1. N2H2's student/non-student ratio is about 9.5/1. Websense claims N2H2 has fewer than 150,000 corporate seats.
Revenues/Seat	Very low; trying to move from advertising model to subscription model.
Monitoring	"N2H2 logging provides an audit trail of Web request information that may be used later in conjunction with configurable reports" (Product overview). "Built-in instant access to individual Web use data." "N2H2 Internet Filtering for ISA Server logs the specifics of every Web request" (White paper). But see the note about the SBA below.
Corporate	At most, less than 10% corporate.

Comments	N2H2 only entered the enterprise market in May 2000 N2H2 recently made its first sale to a federal agency: 6,500 seats at the Small Business Administration. But *Federal Computer Week* (Feb. 5, 2001) says that "Instead of resorting to actively monitoring employees' Web usage and having administrators cull through these reports, SBA relies on the N2H2 software to block employees from accessing inappropriate sites." Blocking sites, without recording the attempt to access them, shouldn't really be considered monitoring.
Monitored Employees	16 million total - 14.5 million students = **1.5 million** non-students

Symantec	SYMC; Cupertino CA; http:/www.symantec.com
Product	I-Gear; Mail-Gear (see below)
Price	"Pricing starts at $2,495 for a one-time licensing fee for 50 simultaneous users."
Seats	Symantec acquired I-Gear from URLabs. A 1998 article on URLabs said it "markets a server-side content management service to 3 million users in nine countries" Symantec acquired the company in Aug. 1999 for $42 million. URLabs marketing material from before the Aug. 1999 acquisition claims "Over 4 Million I-Gear users in 11 countries; 1 Million Mail-Gear users."
Monitoring	Capable of being used as a pure monitoring product: "Organizations concerned about the legal implications of providing Web access but reluctant to tackle First Amendment issues will appreciate I-Gear's unique Audit Mode, a feature that enables user-transparent auditing of unfiltered access. Detailed summary reports can be used to pinpoint policy violations without restricting freedom of access" (Press release). Similar feature: "AutoAlert ... sends e-mail to designated recipients whenever specific Web users violate locally defined acceptable-use policies.... A government agency, for example, could offer unrestricted Internet access with a 'three strikes, you're out' policy for workers by linking I-Gear's Audit Mode and AutoAlert features. "
Corporate	A large percentage of I-Gear sales involves schools, judging from press releases at www.symantec.com. At the time of its URLabs acquisition, "Revenue from sales to businesses have grown 68 percent over the last 12 months, to comprise almost half of Symantec's total revenue"
Monitored Employees	Websense claims less than 2 million enterprise seats for Symantec I-Gear Similar to N2H2 until recently, URLabs I-Gear appears to have been marketed almost exclusively to schools. If we take the figure of 4 million users in mid 1999, and apply N2H2's ratio of 16/1.5, we get about 400,000 non-student users (possibly including some teachers). If we then applied a standard 55% annual growth rate, we would get 900,000 corporate users today. Or, we could take the URLabs 4 million figure, estimate 75% (a bit less than N2H2's current 16:1.5 ratio) of it was educational/home. This would mean 1 million enterprise users in mid 1999. Figure a 50% annual growth rate. By mid-2000, they've acquired .5 million new enterprise users. By mid 2001, they've acquired another .75 million, for a total of 2.25 million. We have to split off the Mail-Gear product; figure the same 4/1 ratio holds; that's **1.8 million** for I-Gear and .45 million for Mail-Gear (see below)

Telemate.Net	TMNT; Atlanta GA; http://www.telemate.net
Product	NetSpective, eSpective, NetSpective WebFilter
Revenues	Telemate was recently acquired by Verso Technologies, for about $30 million in stock Telemate.Net's main business is call accounting software. Telemate's latest quarterly report fortunately breaks out "Internet/integrated" revenues from "calling accounting" revenues. In 2000, call accounting represented over 50% of the business; in 2001, it was over 72%. Revenues from the Internet/integrated products were only $591,000 in the Q1 2001, compared to $1,463,000 in Q1 2000. According to Telemate, "the total Internet/integrated revenue was impacted by the shift in focus from the sale of an integrated solution to distinct Internet and call accounting applications." Thus, the annual revenues from Internet monitoring products really is only about $2.4 million.
Price	The quarterly report says that resellers get discounts of 20%-65%. Also according to the quarterly report, "Substantially all of our license agreements are perpetual. Support agreements are typically for a term of one year and renew automatically upon payment of an annual maintenance fee by the customer. This support fee typically represents 20% of the current list price of licensed products."
Seats	Press releases state that "Telemate.Net solutions have been installed in more than 14,000 customer sites worldwide." This includes the more than 50% of Telemate's business devoting to call monitoring.

Monitored Employees	$2.4 million / $5.25 per monitored employee = **450,000** employees whose Internet activity is monitored with Telemate.Net.

Secure Computing	SCUR; San Jose CA; http://www.securecomputing.com
Product	SmartFilter
Revenues	Separate revenue figures are not available for the SmartFilter product. SCUR total revenues: Q1 2001: $11.2M Q1 2000: $7.5M
Seats	"Secure Computing has more than 4,000 customers worldwide, ranging from small businesses to Fortune 500 companies and government agencies." As noted earlier, it would be good to have a figure we could use as average number of seats at a customer site. If Websense's seats/customer ratio held for SmartFilter, that would mean 2.5 million seats. Websense admits "Various integrations with Unix have driven some limited success in the corporate market."
Monitoring	From a number of reviews, it appears that SmartFilter does not do reporting (and hence, can't really be considered to do employee monitoring) unless if used with Wavecrest Computing's Cyfin Reporter. A March 2001 article reports that "the privately held Wavecrest, a small operation with 8 employees, has grown through partner and reseller links. Wavecrest's revenue has tripled each year and in 2000 totaled about $1.5 million."
Monitored Employees	Because of uncertainty about whether SmartFilter by itself can be considered a monitoring product, and because of the small size of Wavecrest, which makes the Cyfin Reporter, SmartFilter will be treated as part of the Miscellaneous category.

Miscellaneous	
Product	Secure Computing SmartFilter (see above) Raytheon SilentRunner: A March 2001 NewsFactor article reports: "SilentRunner has been sold to nearly 150 companies and government agencies eager to bolster security and tighten their control of company secrets and assets. Still, only a couple of companies -- security snoop TruSecure and the consulting firm of Deloitte and Touche -- have admitted using the program, which ranges in price from US$25,000 to $65,000 per copy." According to Wired News, SilentRunner was designed to "answer the insider threat," which would put it squarely as an employee monitoring product. Apart from the two known customers, "not one organization, public or private, had admitted to buying SilentRunner.... Both companies provide security services to client companies. No organization has admitted to using SilentRunner to monitor its own employees.... TruSecure spokeswoman Susan Lee said the company's clients -- it provides constant monitoring to nearly 400 companies -- have asked not to be identified for fear hackers will be tempted to infiltrate SilentRunner-protected networks just for sport." There are dozens of other products from smaller companies, and new companies frequently enter the market. For example: 8e6 (formerly Log-On Data) X-Stop, Adavi Silent Watch, eSniff, Trisys Insight, SpectorSoft Spector/eBlaster, WebRoot WinGuardian, WinWhatWhere Investigator, Actis NetIntelligence, GameWarden, Cerberian, Biodata I-Watch, Open Systems Private I, ICaughtYou.com, computer-monitoring.com, Fatline, FutureSoft DynaComm i:filter, Pearl Echo, PureSight, BigBrother, SpyTech SpyAgent, ICUSurf, Sequel Internet Resource Manager, etc.
Revenues	A sample data point: 8e6 Technologies, makers of X-Stop, formerly Log-On Data Corp. Used by schools as well as by corporations. In August 2000, 8e6 was named to a Deloitte & Touche "Technology Fast 50" list, to qualify for which a company must have been in business a minimum of 5 years, had 1995 revenues of at least $50,000 and 1999 revenues of at least $1 million. But X-Stop may only do monitoring/recording when used in conjunction with NetSpective?
Monitored Employees	Adavi, makers of Silent Watch. Sells for $200, and can monitor up to 4 computers; each additional seat is about $35. The *Wall St. Journal* (March 7, 2000) said that Adavi had sold more than 1,000 copies of the (then) $159 program, which it started marketing in July 1999. Many of these sales were likely to parents and spouses. 1,000 copies sold July through March means about 125 copies per month. Assuming steady sales since July 1999, that's maybe 3,000 copies. Assume each one is used to monitor 4 employees? Some

	aren't for corporate use; some will be, and will have purchased additional seats; figure these cancel each other out. About **15,000** monitored employees? WinWhatWhere Investigator: the same *Wall St. Journal* article (March 7, 2000) says more than 5,000 licenses had been sold since August 1998. This is about 250 per month, or about **9,000** copies sold. Again, likely a large number of non-corporate users. eSniff: *Red Herring* (April 3, 2001) reported that "eSniff has sold about 70 customers on its product." Actually, there are two products: the 1100, which can monitor 1,000 users ($10,000), and the 1000 which can monitor 100 users ($5,000). "SpectorSoft has sold **35,000** copies of its spyware" (*Time*, July 2, 2001). As noted earlier, when Australian e-mail-filtering company EmUTech was acquired by SurfControl in December 2000, EmUTech was said to cover **45,000** users. It might be fair to estimate about 30,000 employees monitored on average by each of the smaller/newer companies. Figure about three dozen of them; that's 1.08 million. Raytheon SilentRunner is the big unknown, it's not clear whether to include Secure Computing SmartFilter, so just say **1.2 million** for miscellaneous.

Appendix C: E-mail Monitoring

Totals for E-Mail Monitoring, Worldwide

MIMEsweeper	7.25 million
Tumbleweed MMS	1.5 million
SurfControl E-mail Filter	1 million
Elron IM Message Inspector	.95 million
Symantec Mail-Gear	.45 million
SRA Assentor	.1 million
Miscellaneous	.75 million
Total	12 million

As noted above, the distinction between Internet and e-mail monitoring is somewhat artificial. As another example, we're considering Baltimore's MIMEsweeper product line to be entirely devoted to e-mail monitoring, yet one of its components is WEBsweeper. Similarly, Tumbleweed has a Web Filter product. However, it's possible that these products are used primarily for the increasingly common e-mails formatted as HTML pages, and for web-based e-mail such as Yahoo! and Hotmail.

Baltimore Technologies	BALT; Dublin, Ireland; http://www.mimesweeper.com
Product	MIMEsweeper, MAILsweeper, PORNsweeper, WEBsweeper, SECRETsweeper, e-Sweeper, MAILpreserver
Revenues	The MIMEsweeper line of products is just one part of Baltimore's business. Total Baltimore revenues were $33 million in 1Q 2001, down from $40 million in 4Q 2000. Baltimore doesn't release separate revenue figures for MIMEsweeper. MIMEsweeper was acquired as part of Content Technology in September 2000. A Baltimore FAQ on the acquisition states: "Content Technologies' revenues for 6 months ending July 31, 2000 amounted to £9.2 million with some 42% of revenues derived from U.S. operations." This represents annual revenues of about $25 million.
Seats	At the time of the Content Technologies acquisition, Baltimore stated that "Over 6,000 customers and 6 million users throughout the world currently use Content Technologies MIMEsweeper to protect against business and network integrity threats" In November 1999, Content Technologies claimed 4 million users of MIMEsweeper. "MIMEsweeper products have over 6 million users worldwide. There are currently 4.4 million users of

	MAILsweeper and 1.2 million users of WEBsweeper version 3" (Product Info Bulletin, Nov. 2000). Because of the WEBsweeper product, some of the employees covered by the MIMEsweeper family really ought to be moved over to the web-monitoring category. On the other hand, it is possible that WEBsweeper is largely used for HTML-based e-mail, and for web-based e-mail (e.g., Yahoo mail, Hotmail). Right now, the MIMEsweeper home page states that "Over 10,000 customers and 10.5 million users worldwide have selected solutions from the MIMEsweeper family of products to implement their information security policies." "Baltimore now has over 8,000 customers worldwide using Baltimore MIMEsweeper with approximately 445 new customers signed in Q1" (Press release). If the correct number of customers is 8,000, then the average customer site has 1,300 seats. If the correct number is 1,000, then the average customer site has 1,050.
Monitoring	"A strong defense involves proactively monitoring employee e-mail to ensure that it is free from trade secrets or litigious language" (White paper).
Monitored Employees	We could just take the 10.5 million figure, and be done with it, but we need to remove some percentage of employees whose companies are using MIMEsweeper mostly for external threats (spam, e-mail viruses, etc.) rather than the "internal threat" which is the target of employee monitoring. In the absence of any other information, we'll have to go with the 70% figure from Websense (the percentage of their customers who install the Reporting module, and therefore can be said to do monitoring), and apply that: 10.5 million * .7 = **7.25 million** employees monitored with MIMEsweeper.

Tumbleweed	TMWD; Redwood City CA; http://www.tumbleweed.com
Product	Messaging Management System (MMS)
Revenues	Tumbleweed revenues have fallen from $12.4 million in Q300 to $8.2 million in Q400 to $4 million in Q101. This may be due merely to Tumbleweed's revenue-model change. However, Tumbleweed has also recently laid off 20% of its staff. Tumbleweed acquired Worldtalk (then WTLK) in late 1999. At the time, Worldtalk's year-to-date revenues were about $4.9 million (Press release). Worldtalk remains a wholly-owned subsidiary. Tumbleweed's own revenues for the first 9 months of 1999 were $3.4 million (press release, Oct. 19, 1999). It is therefore reasonable to say that Worldtalk's e-mail-monitoring business would represent about 60% of the revenues of post-acquisition Tumbleweed. (Tumbleweed's other main product line is the secure-channel Integrated Messaging Exchange.)
Seats	Worldtalk's WorldSecure product appears to be a reasonable proxy for MMS: "For people interested in WorldSecure, Worldtalk's award-winning e-mail management solution, this technology is still available as part of the newly introduced Tumbleweed Messaging Management System." A Feb. 2000 statement claimed "currently over 1,000,000 end users of WorldSecure/Mail." At the time of the Worldtalk acquisition, Tumbleweed noted that "Worldtalk brings to Tumbleweed more than 400 customers, including Chevron, Nike, Time Warner, U.S. Dept. of Energy, Blue Cross, Glaxo-Wellcome and GE Capital." UPS is a major MMS client.
Monitoring	"MMS CONTENT MANAGER scans messages and attachments for specific words or strings of words. When a policy violation is detected, MMS can take a number of actions, such as block, quarantine, archive, or defer delivery. With MMS ACCESS MANAGER, companies can set policies that restrict e-mail from certain senders or to certain recipients. For example, policies can block inbound messages from known problem or spam domains, or prevent confidential information from being sent to a competitor's e-mail domain. MMS VIRUS MANAGER uses integrated server-based anti-virus software from Network Associates to detect and optionally clean or strip infected attachments in both incoming and outgoing messages. Tumbleweed Message Monitor allows organizations to archive all or selected messages to an external device, such as an optical jukebox. Messages can be tagged with information such as violation type and retention period prior to archiving. Tumbleweed Message Monitor provides Web-based reviewer tools for performing queries and running reports. Tumbleweed Web Filter provides URL filtering and monitors HTTP and FTP traffic for inappropriate content, viruses, and malicious mobile code. Tumbleweed Web Filter can also monitor the content of Web-based e-mail and message board postings" (Annual Report, 2000). Not all of this is employee monitoring: as the quote above shows, MMS is also used to control spam and viruses. Offers ability to "archive e-mail of all or selected employees for sampling, periodic review, and evidence of supervision; Identify and archive messages that appear to be making promises of guaranteed results or other prohibited statements."

Monitored Employees	It seems like it should be easy to figure out the number of employees whose e-mail passes through Tumbleweed MMS because, in early 2001, Tumbleweed stated that "Committed message traffic under contract at year-end reached 1.48 billion messages, compared to 1.29 billion messages at the end of Q3 The average white-collar worker is reported to receive about 40 e-mail messages at the office every day. Figure that the employee replies to perhaps 1/4 of these, for 50 messages a day (Microsoft reports its 39,100 employees deal with about 4.3 million messages per day, or a little over 100 per employee per day.) With about 220 work days per year in the U.S., that's 11,000 messages per employee per year. Divide Tumbleweed's 1.48 billion messages by 11,000, though, and you come up with only about 135,000. It turns out that "committed message traffic under contract" means something entirely different. So let's try a different technique. 1 million users of WorldSecure/Mail in Feb. 2000 would, with a usual 50% annual growth rate (though Tumbleweed's revenues haven't grown that way recently), put the number of users at about 1.75 million. On the other hand, if we take TMWD revenues of about $18 million a year (it's a little unclear right now because of a change in the revenue model), figure 60% of this represents MMS (see above), we get about $10.8 million MMS revenues. Using our standard $5.25 per monitored employee, that would also give us about 2 million users. However, MMS is also being used for virus elimination and other non-monitoring purposes, so we need to subtract something. As with MIMEsweeper, the best thing is to figure that only about 70% is really employee monitoring, with the result that about **1.5 million** are monitored under MMS.

Miscellaneous	
SRA Assentor	"Our Assentor software is the market-leading e-mail screening and archiving solution for the financial services industry; our client base of more than 75 firms, with over **100,000** seats installed, represents every size and segment of the industry, including retail and institutional brokerages as well as insurance firms" (Annual Report, 2000).
SurfControl E-mail Filter	4.75 million - 3.75 million (based on 3:1 ratio) = **1 million** (see above)
Elron IM Message Inspector	1.9 million / 2 = **.95 million** (see above)
Symantec Mail-Gear	2.25 million / 5 (based on 4:1 URLabs ratio) = **.45 million** (see above)
Others	MailMarshal; Blue Sky E-Post/Gatekeeper; MicroData Cameo amd Melia; xVault xvMail; Lyris MailShield; other software used for broker monitoring under SEC and NASD regulations; other Microsoft Exchange add-ins; other spam/virus filters also sometimes used to examine employee outbound e-mail; etc.: **.75 million**