

PEER-REVIEWED JOURNAL ON THE INTERNET

Understanding the Privacy Space

by Benjamin D. Brunk

Abstract

Understanding the Privacy Space by Benjamin D. Brunk

This paper reports on an ongoing research project focusing on privacy tools, and services available on the Internet. A detailed examination of 133 different privacy-related software tools and services rendered a list of 1,241 features relating to privacy. Based on the data gathered, the ongoing work is to formulate a framework to describe this "privacy space" using grounded theory and content analytic techniques. Here, we discuss some of more interesting preliminary findings garnered from a descriptive statistical analysis of the raw data. This paper discusses what can be learned from a user-centric analysis of this increasingly important class of software tools.

Contents

[Introduction](#)

[Methodology](#)

[Results](#)

[Discussion](#)

[Conclusion](#)

Introduction

This research focuses on the "Privacy Space" - a loosely defined collection of software systems and online services devoted to protecting people's privacy in cyberspace. The problems related to online privacy have received a great deal of attention in the popular press, in academia, and in public policy debates. A wide variety of solutions have been devised in the attempt to bolster online privacy in the face of numerous different threats and potential abuses of information technology. While technology is never going to solve all of our problems, it is useful to illuminate what successes have taken place and what more can be done. To date, there has never been a thorough study of the state of the art in privacy tools, systems, and services. Much analysis has taken place, but we lack a clear and concise means for discovering what problems have been addressed, their general success or failure, and what issues have been overlooked and may be fertile ground for new research.

There are many people and organizations trying to use technology in an effort to enhance security and privacy online. Some have examined very specific problems, while others have tried to be more all-encompassing. A few solutions are well known and very popular amongst Internet users. Others remain obscure and underutilized. This research project investigates the realm of privacy (and to a lesser extent, security) tools, systems and services, from the end user's perspective. Encryption tools, anonymous and pseudonymous proxies, virus and Trojan horse detection systems, personal firewall tools, secure deletion utilities, cookie managers, Web bug detectors/filters, checksum tools, authentication and trust systems, intrusion detection systems, backups, and a host of educational or awareness raising products all have privacy features built into them or play a significant role in helping to protect one's privacy. These solutions vary widely in application, user involvement, and level of expertise required. Finding the relationships between the solutions that have been tried will improve our understanding of the overall problem. A general research question for this work is: What are the critical dimensions for a framework to describe systems that include privacy-enhancing features?

Privacy

Privacy has always been a profoundly difficult thing to comprehend. Privacy is a matter of intellectual and philosophical thought and retains few tangible characteristics, making it resistant to simple explanation. In just over 100 years, the concept of privacy has evolved into a broadly defined concept that ties together a number of different forms of resistance against intrusion upon the individual (Schoeman, 1984). People claim a right to privacy for an enormously broad range of issues, including surveillance and mail interception, sexual and contraceptive practices, and financial transactions. Medical records are another recent subject of discussion (Flaherty, 1989), as well as one's behavior while using the Internet (Hoffman et al., 2000). Privacy is an important subject because it affects the way we feel and act. Whether we are conscious of it or not, privacy has very real implications in our lives, despite its ambiguous nature. Whether we approach privacy as a social construct or a matter of law, definitions of privacy abound. It is hard to come up with a single, all-encompassing definition for all the contexts in which privacy is discussed. The "right to enjoy life and be let alone" (Cooley, 1888) probably comes the closest. Another might be having the ability to control one's own "humanistic property" (Mann, 2000). Similar to other desirable and equally ambiguous commodities such as freedom or liberty, privacy comes at a cost. Privacy is balanced with other core values such as free speech, social interaction, efficiency, safety, and accountability. Everyone needs privacy, but people have never sought absolute protection of their privacy. In addition, there is no "one-size-fits-all" remedy or equation that decides how it should be balanced with other goods. Our privacy needs change almost constantly in response to our desire to interact with one another and social mores and institutions affect privacy expectations. Society has a strong influence on our attitudes towards privacy and on how much (or how little) privacy individuals can attain.

The question of how human values, ethics, and morals relate to software design is of growing importance in the HCI community. Friedman and Kahn (2002) discuss these issues in detail. Most notably, they question what values count, when values are relevant, and who is it that is deciding what moral and ethical standards a given design will follow. Friedman and Kahn describe three ways in which values become implicated in design and follow on by discussing several approaches for consideration of human values and ethics in design. Finally, they describe a number of human values with ethical import including human, welfare, property rights, freedom from bias, and privacy.

The privacy space is an exemplar of a human value (the desire to control personal information flows) instantiated via the design of software systems and services. Here, we see how privacy, a subject with ethical import, relates to system design and usability. Systems may be designed from the outset or modified by users to enhance usability and help them realize their goals and intentions, including those related to privacy. Thus, for the purposes of this research, we define "online privacy" as having the ability to control information leaving you while online, and being able to exercise that control consistent with your values. In a passive sense, privacy is also about being able to control unwanted intrusions. We claim that people seek designs that provide easy and effective ways to achieve online privacy, verify that they have done so, and monitor effectiveness.



Methodology

In previous work, privacy has most often been examined from a security perspective based on "threats" and "intrusions" with a goal of producing algorithms or comprehensive solutions. Also common is the discussion of privacy in terms of policy and law, with an eye towards "fixing" laws that fail to prevent undesirable information exchanges or creating completely new laws and proscriptions against technologies or techniques that can be used to invade people's privacy. This research differs from those models in that privacy will be addressed from the perspective of the individual and with a focus on the human-computer interface (e.g. giving people personal control over their own interpretation and immediately applicable version of privacy). The intent is to gain some kind of perspective in order to better see what issues have been addressed as well as spotting the remaining gaps.

To those ends, the approach of this study is to identify and then analyze a broad sample of tools, systems and services, collectively referred to as "solutions." A wide variety of freeware, shareware, adware, spyware and demonstration packages (a.k.a. crippleware) as well as many different services offered via the Web and the Internet in general constitute the inputs to this analysis.

Content and Features Analysis

Content analysis is very much a grounded theory approach (Glaser and Strauss, 1967). Krippendorff (1980) describes Content Analysis as a "research technique for making replicable and valid inferences from data to their context." We want a methodology that is objective, systematic and replicable. A large portion of creating the framework is in devising a reliable and replicable coding schema capable of adequately describing the features of the tools and services being observed. A central idea in content analysis is that many observed pieces of data are classified into a set of content categories (Weber, 1990). In terms of text, words, phrases or other units are classified into categories. Entries in each category are presumed to have the same or similar meanings. In this study, we are interested in software features instead of words, but the same principles apply.

A software feature is a capability for completing a certain task that has been designed into a system. Privacy features are those that offer some sort of privacy-related functionality to the user. A privacy feature need not be motivated by design goal, it only matters that the resulting capability somehow relates to privacy. It is often found that tools designed for one purpose are later adapted for other purposes.

A trial features analysis was conducted on a small subset of samples from the population of privacy space solutions as part of an earlier study (literature reviews and background preparatory work for the author's dissertation proposal). To gather samples, the pilot survey used two different Web-based software download sites that include privacy and security tool categories. The results indicate that it is possible to discern and name privacy features in software applications and Internet-based privacy services. That work has led to the identification of five role categories that describe privacy solutions in terms of how they protect privacy - prevention, detection, response, recovery, and awareness. The first four roles were adopted from the literature dealing with institutions and organizations that require large-scale security systems, tools and policies (Schneier, 2000). Based on the conclusions of the pilot study, Schneier's four categories with the inclusion of a fifth relating to general privacy knowledge and awareness make a useful starting point as an appropriate and sufficient means for classifying privacy solutions based on their features. These categories are defined in [Table 1](#).

Table 1: Role Categories

Awareness	Anything that conveys information without requiring the user to act. Awareness features are informative and help you monitor what is going on.
Detection	Tools or features that scan or actively look for potential problems. Often, detection tools are always running in the background; a virus scanner is one example.
Prevention	A feature or tool that is used as a precaution. Encryption or digital signatures are preventative in nature, they usually only run when needed. Shredding sensitive documents is also a good example.
Response	Taking action after a problem has been detected is a response. Cancelling your credit card after it has been stolen, or blocking incoming network traffic from certain IP addresses are examples of a response.
Recovery	Features and tools that help you get back to normal. Restoring to the last known good state, patching bugs that allowed intruders to gain unauthorized access, and re-installing corrupted files are examples.

It is difficult to separate privacy features from security features, and there will a great deal of overlap between the two because the same features that are useful for protecting against security intrusions are also good at protecting privacy [1]. There is also some subjective interpretation required of the researcher as to what constitutes a single "feature." Once a set of features has been identified and named, recognizable patterns begin to emerge. Haas and Grams (2000) offers an example of a successful features analysis using Web site content to create a taxonomy of page type classifications as a means of understanding and categorizing the purpose of Web sites or individual pages. The questions they ran into were similar - "What is a Web page?", "Is it reasonable to assume that there are enough common elements across Web pages to warrant constructing a single typology of page and link types that applies to them all?" The

current study utilizes a similar bottom-up approach at a classification scheme for privacy solutions based on their purpose. With privacy solutions, however, it is more obvious that we are interested in a finer grained analysis of features rather than just whole solutions, and that there are enough commonalities among solutions for the analysis to be successful.

The Sample

In total, 133 solutions were evaluated in the study. Candidate examples are those reported to include privacy or security enhancing features. The goal is to cast a wide net and examine the population of privacy solutions as exhaustively as possible. Other studies that have analyzed Web content (e.g. Bucy et al., 1999) sampled a population of Web sites. Due to the sheer number of the sites in the sampling frame (5,000 Web sites were identified, 500 were selected for evaluation), only 10 percent were actually examined. The privacy space is quite a bit smaller, but the problem is the same. Because of the time it takes to analyze each solution, we are not able to perform an exhaustive analysis on the population.

Samples for analysis were identified using the following methods:

- Web portals specializing in providing software tools and utilities for the Internet;
- Privacy Web sites such as epic.org, eff.org and privacilla.org that recommend tools and services;
- Web sites of vendors;
- Organizational Web sites (e.g. W3C, CERT);
- Software stores both online and offline;
- News articles;
- Journal articles, and;
- Word of mouth - solutions brought to my attention or recommended by colleagues.

Procedure

Once a solution became part of the sample frame, it was evaluated by locating its home Web site and reading about it as well as by trying to use it. This usually meant downloading and installing a program or testing out an online service. Most solutions were fully-functional applications that had 15 or 30-day usage restrictions enforced by "time bomb" logic that would deactivate the application if it was not registered before the time limit expired. Others were freeware, open source, or relied on the honor system for user registration. In no case was a solution actually purchased as there were no funds to cover licensing or subscription fees. As a result, there were some cases where the evaluation relied solely upon published help files or example interfaces (screenshots) as well as Web site promotional information. These specific cases proved harder to evaluate, but were few in number and still provided valuable data.

For each solution, the goal was to ascertain what privacy features were offered and then describe them. Each solution had many different features, but normally only a few of those related directly to privacy. Each feature was described in a short paragraph focusing on its functionality and user interface characteristics. For example, if the feature could be turned on an off via a checkbox widget, that information was included in the description along with whether the checkbox was selected or not selected by default. Each feature description also included a screenshot and a tick mark indicating whether it made significant [2] use of graphics or not.

In addition to the privacy features and their descriptions, the following information was also collected:

- Name of solution;
- Approximate year first available;
- Architecture of solution (client, server, standalone tool, built-in feature, or proxy);
- Screen size;
- Version;
- Cost;
- Operating system;
- Open source/Proprietary;
- Current availability;
- Memory resident/Runs as needed;
- Standardization/De facto standard;
- Role of solution (Awareness, Detection, Prevention, Response, or Recovery, if possible);
- Role of each feature (Awareness, Detection, Prevention, Response, or Recovery);
- Significant use of graphics in feature implementation;
- Name of producer;
- Web site URL;
- Estimated size of producer's organization;
- Country of producer;
- City and state of producer, and;
- E-mail address of producer.

A lot of data was collected because no one has tried to do a features analysis with such a narrow focus before. It was not known from the beginning what items would prove interesting or lead us to a better understanding of the privacy space. Our results focus on the more enlightening trends and patterns identified from the sea of data collected.



Results

The list of 133 solutions is too lengthy to present here, refer to <http://ils.unc.edu/~brunkb/dissertation.html> for more information about them. [Figure 1](#) shows the breakdown of the approximate year that the solutions we sampled were released:

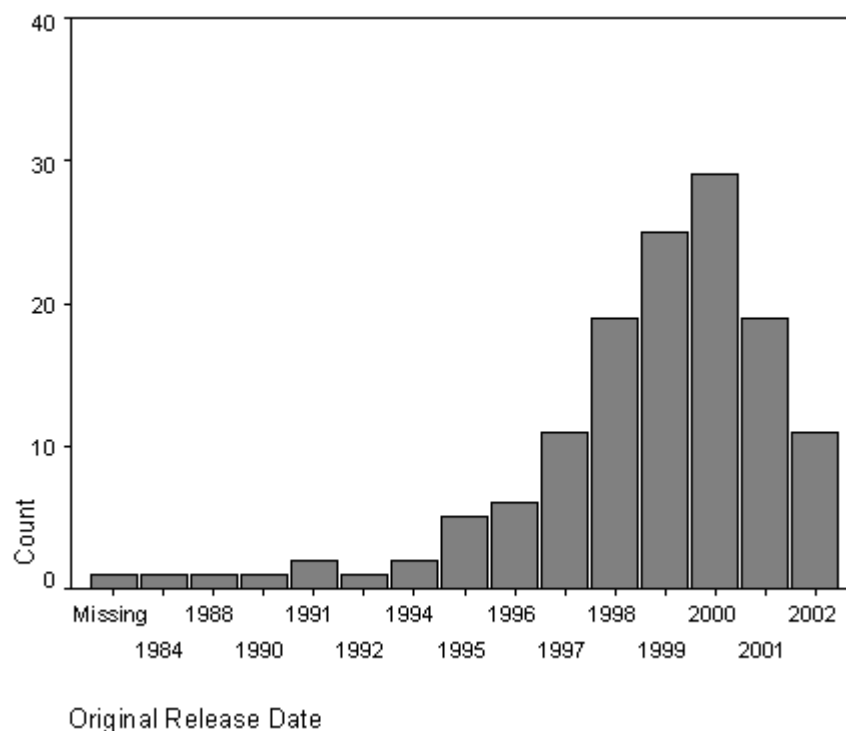


Figure 1: Solution Release Date

In [Figure 1](#), year data is heavily skewed towards the late 1990s with a distinct upward trend peaking in 2000. The study was undertaken in April of 2002 and new privacy tools are hitting the market all the time, so the current year will continue to grow. This is only a sampling of the solutions available each year, thus the counts are not exhaustive.

Another data point that was recorded deals with the architecture of the solution. Here, architecture refers to what kind of system the feature appeared in. Was it part of a server or Web site? A proxy? A plug-in module or built-in feature of a larger application? Or was it a standalone application that runs independently of other applications?

Table 2: Tool Architecture

Architecture	Frequency	Percent
Server	7	5.3
Proxy	6	4.5
Standalone tool	107	80.5
Plug-in	1	0.8
Built-in feature	4	3.0

Web site or Web-based	1	0.8
Not Applicable	4	3.0
Not recorderd	1	0.8
Other	2	1.5
Total	133	100.0

Table 2 reveals that 80.5 percent of the solutions in the sample were standalone applications. Very few were categorized as a server (5.3 percent), or proxy (4.5 percent). Only three percent were described as a built-in feature and 1.5 percent fell into the category of "other" meaning that it was not clear what they were. Web-based services and plugin modules both made up only 0.8 percent of the sample.

Looking at the solutions by their country of origin, we see that the privacy space looks much like any other class of software and services. As **Figure 2** indicates, the majority of the samples came from the United States, but many other countries were represented, some of them quite strongly, especially Germany, Russia, Canada, and the U.K. Interestingly, a significant number of solutions (4.5 percent) could not be categorized by country; no such information was given or could be discerned, even using techniques such as a "whois" lookup on the domain name of the company or individual.

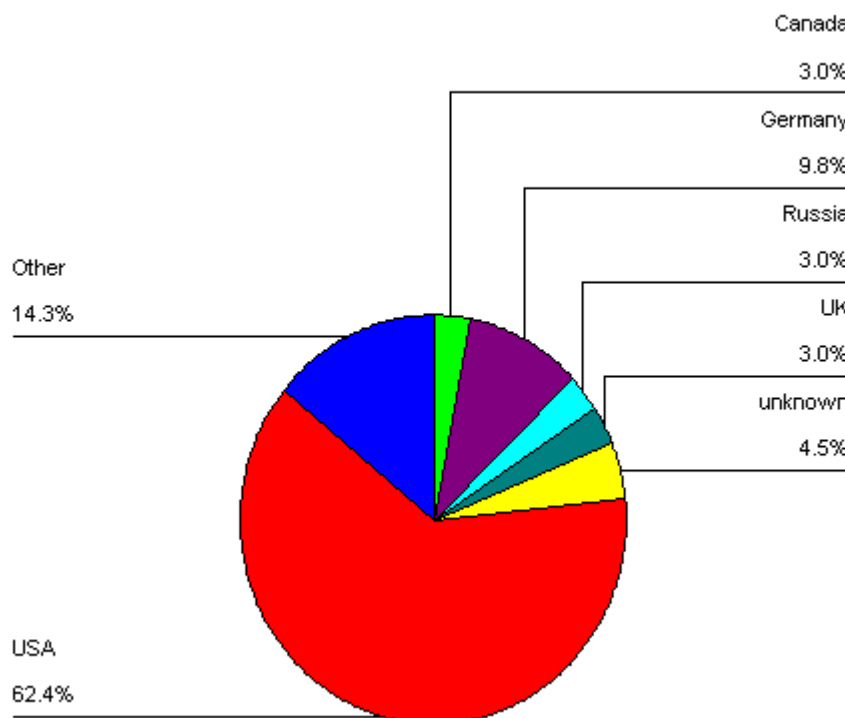


Figure 2: Principal Nationality of Solution Provider

Another item of interest was the size of the organization that produced the solution. We must use the term organization a bit loosely though because as [Figure 3](#) indicates, the privacy space is hardly organized - lone individuals were responsible for a great number of the solutions. Unfortunately, obtaining this data was hit or miss. It turned out to be very difficult to figure out the size of an organization just from its Web presence unless it happened to be a well-known company. In some cases, the necessary information was published right on the Web site. In other cases, the issue was left intentionally vague or misleading.

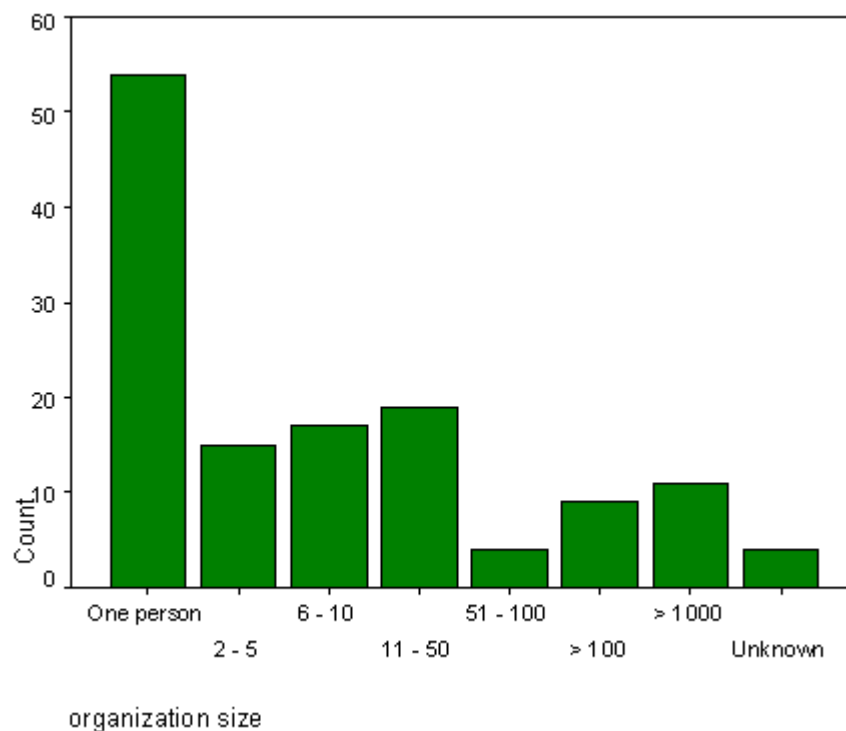


Figure 3: Organization Size Estimates

[Figure 4](#) refers to type of license or business model of the solutions in the sample. In all, 109 solutions, or 82 percent, were found to be proprietary source while the remaining 24, or 18 percent, were designated as open source. This may or may not be an accurate portrayal of the entire privacy space, since many of the programs and services were subscription-based.

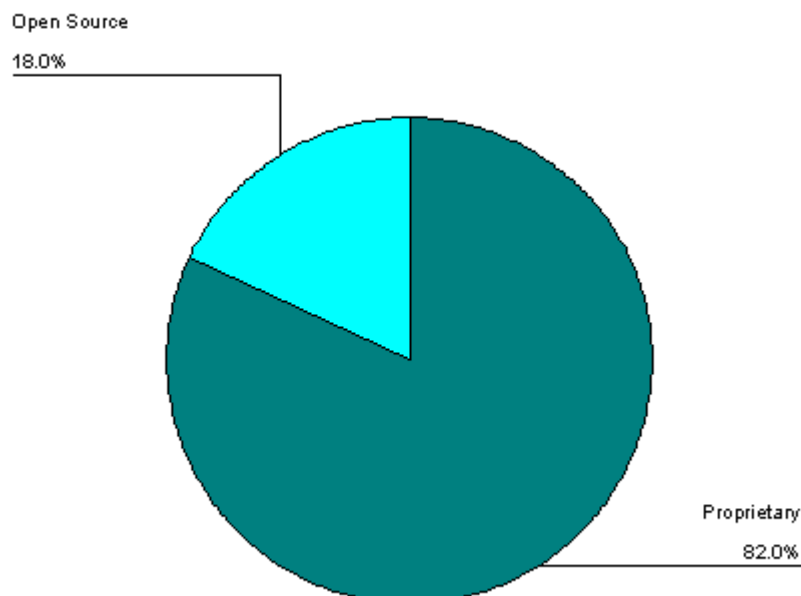


Figure 4: License Type/Business Model

Microsoft Windows was by far the most common target platform (60.3 percent of cases, [Figure 5](#)). But Linux and several different Unix platforms (generically referred to as Unix) were well represented. Solutions for MacOS and OS X fell within the "Other" category, and the little-known BeOS even appeared. Some solutions worked with any operating system as they were either Web-based, Java applets, or a service (e.g. certificate authority or privacy seal program) that did not rely on client-side software.

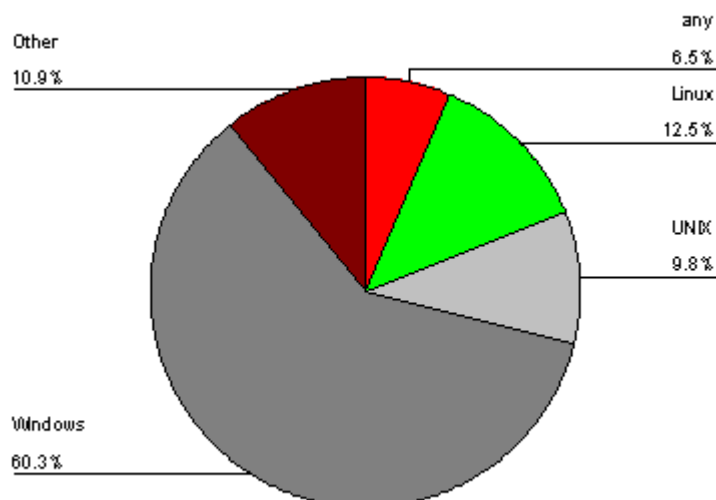


Figure 5: Operating System of Sample

In terms of cost, [Figure 6](#) relates the story to us. The majority (68) of the solutions examined were freeware. Several of the examples were open source and were downloaded as a tarball or rpm. Many of the free programs had licenses stipulating that the package was free as long as it was used for non-commercial, home use. We defined "cost" as the amount an individual would have to pay for one year's use of the solution, so although many of these were recorded as "free", they were only cost-free if used in certain narrow capacities. This business model seeks revenue from commercial uses and hopes for a viral marketing effect. Essentially, these companies are writing off single-user licenses as an advertising expense.

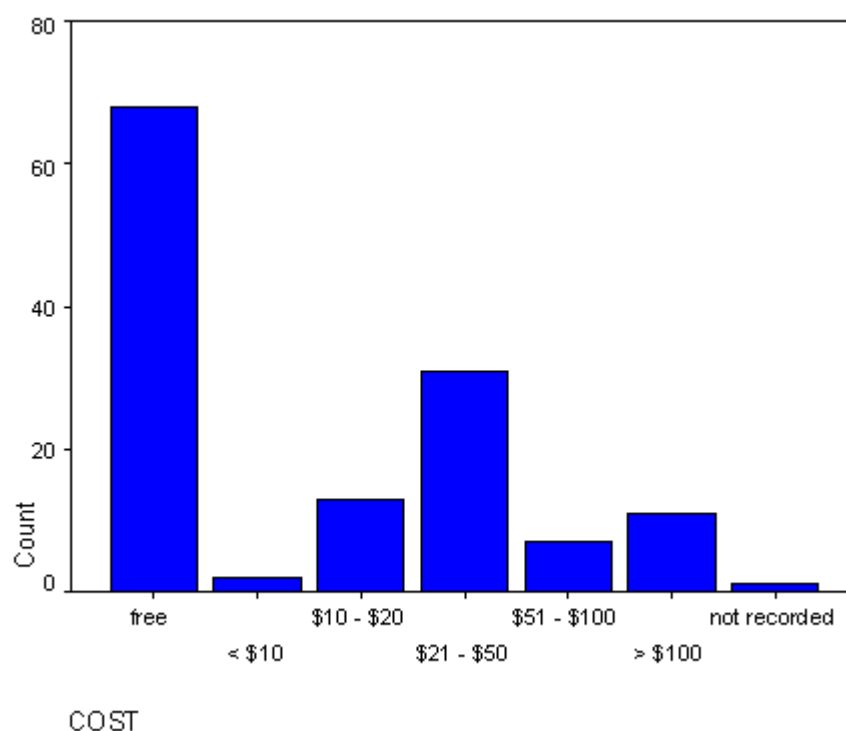


Figure 6: Solution Cost

Among the non-free solutions, some solutions incurred a one-time fee, while others were subscription-based, so quarterly or monthly fees were calculated for a whole year. Site licenses and other group licensing models or usage fees were not recorded. The most frequent price range was the US\$21-50 range with 31. Surrounding that range, the US\$10-20 and >US\$100 categories were next in frequency (13 and 11, respectively). Finally, seven of the solutions fell within the US\$51-100 category, and only two in the <US\$10 category leaving one whose cost information was not recorded.

One of the items of interest during the design of this study was of standardization and de facto standards. For our purposes, a solution was a "standard" if it relied heavily on the work of a major standards body such as the W3C, for example a tool for creating P3P policies. Other tools were deemed a "de facto" standard in the sense that it, or its method of doing something, has been widely adopted. The encryption tool PGP is one example

of a "de facto" industry standard [3]. [Figure 7](#) illustrates how few of the solutions that we sampled fit our description of a standard.

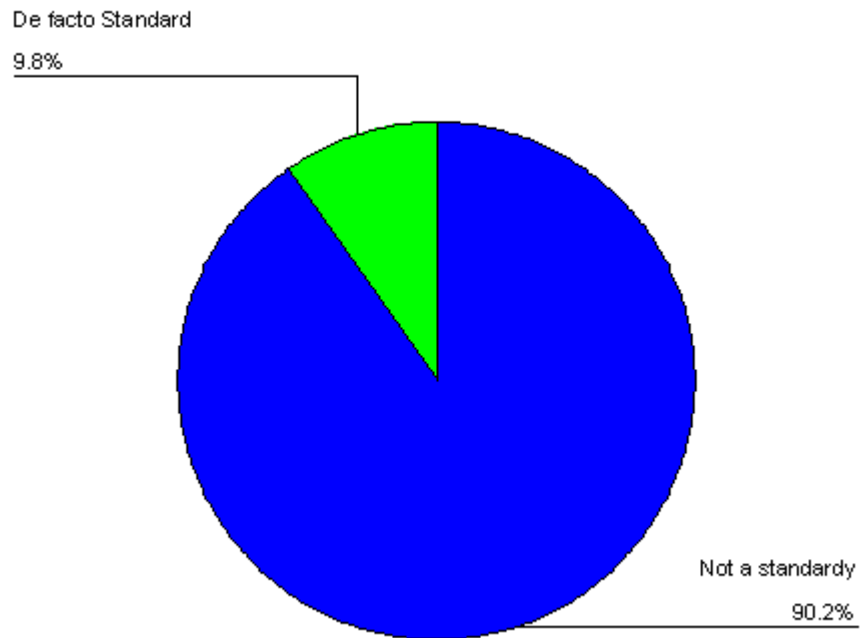


Figure 7: Standardization

Availability was another item of interest when the study was being designed because the dot-com crash was going on; it was assumed that many solutions would suddenly disappear. All but two of the solutions were still available at the time they were analyzed ([Table 3](#)). This data point will be more interesting in a longitudinal type study where we revisit the same solutions at a later date. It is too soon to try and interpret this data or recognize any trends.

Table 3: Solution Availability

Availability	Frequency	Percent
No Longer Available	2	1.5
Still Available	131	98.5

As this research is being conducted under the umbrella of human-computer interaction, we tried to examine some of the user interface characteristics present in our sample.

Table 4 is focused on what interface characteristics were observed in our sample. Nine percent of the solutions were command-line oriented programs. Most of the others involved some size GUI dialog, either with or without a "tray icon" (which is a feature unique to the Windows operating system). The resizable main dialog was most common, covering 19.5 percent of cases, while the small, un-resizable dialog was found in another 16.5 percent of cases. The dialog and tray icon cases were found in over a quarter of the sample. The "other" and "not applicable" categories came into play where services (e.g. proxies, seal programs) or add-ons (e.g. plugins) were encountered.

Table 4: Interface Characteristics

Description	Frequency	Percent
Command Line	12	9.0
Resizable Dialog	26	19.5
Small Dialog	22	16.5
Medium Dialog	14	10.5
Large Dialog	1	0.8
Small Dialog + Tray Icon	9	6.8
Medium Dialog + Tray Icon	9	6.8
Resizable Dialog + Tray Icon	16	12.0
Not Applicable	2	1.5
Not Recorded	1	0.8
Other	21	15.8
Total	133	100.0

Two-thirds of the solutions were not memory resident programs or always-on type services (**Figure 8**). The remainder were installed to run whenever the computer boots, or whenever someone logs in. Services such as proxies, anonymizers, or anything that involved a website were also considered to always be running.

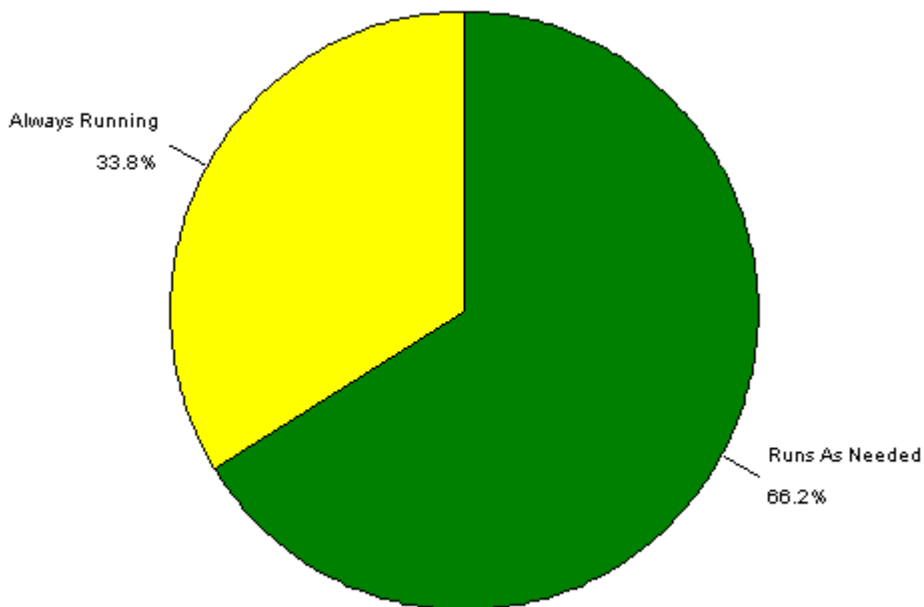


Figure 8: Runtime Characteristics

In all, 1,241 total features were identified and described. [Figure 9](#) shows the breakdown of feature counts among solutions with the largest number having only one identifiable privacy feature. Solutions with four or five privacy features were the second most common in number.

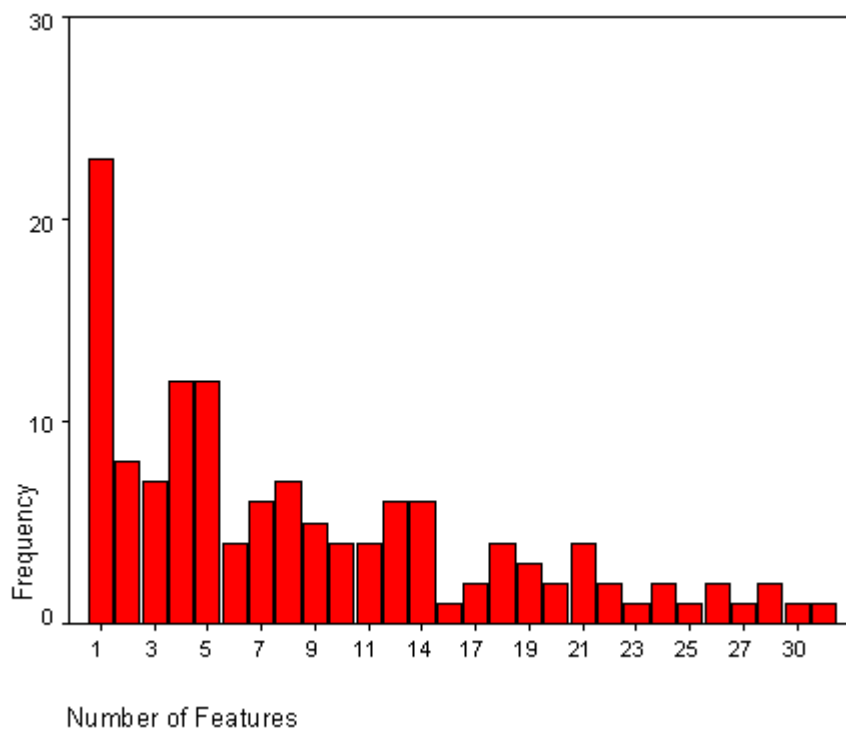


Figure 9: Solution Feature Counts

In addition to user interface characteristics such as screen size, we were also interested in what role graphics played in the design of these solutions. During the features analysis, each feature had a description written about it as well as a notation about whether or not it made significant use of graphics. Clearly, graphics were not common (Figure 10). That is not to say that the GUIs were not graphical. We were looking for anything beyond the standard interface widgets that convey information through the use of information visualization techniques, such as a progress bar or progress meter.

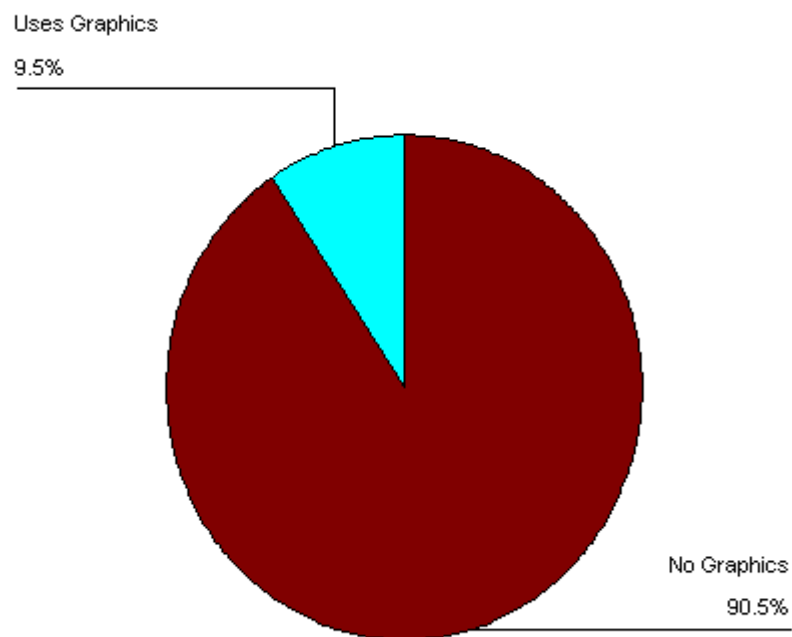


Figure 10: Novel Interface Features (Graphics)

Each solution and each feature was categorized by its perceived role. This categorization took place before the features were analyzed. The idea was to make an educated guess about what role the solution fit into and then see if the features analysis corroborated the initial assumption. Solutions could be categorized into more than one role. The results (Figure 11) indicate that the prevention category is dominant among the five. There were very few solutions categorized as being involved solely with recovery from intrusions.

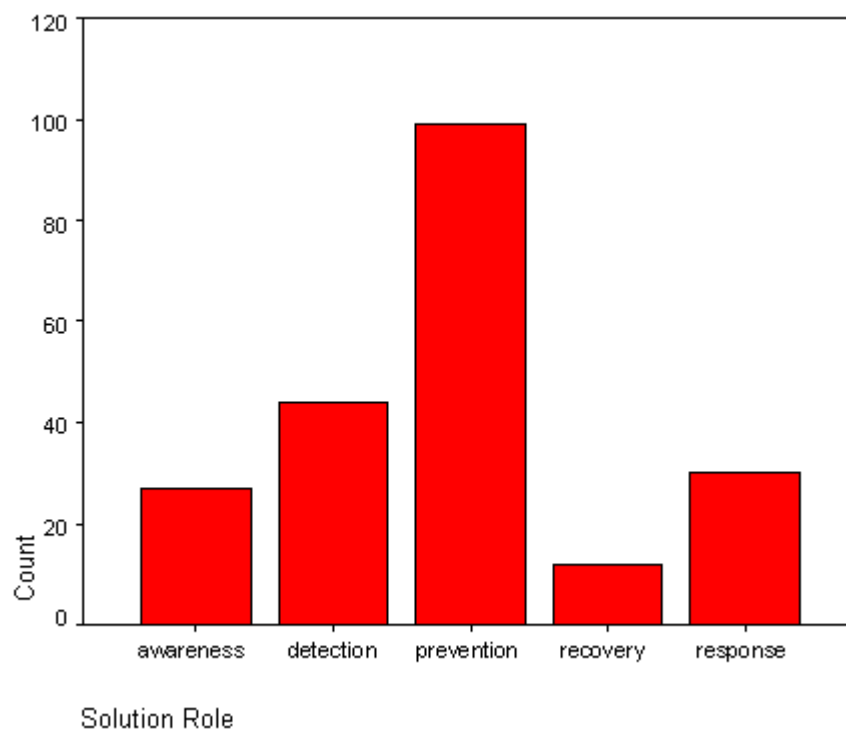


Figure 11: Solution Roles

Contrast those categorizations with the categorizations of individual features as shown in [Figure 12](#). Features could also be placed in multiple categories, however, most were placed in only one. Here, prevention is even more dominant. Solutions assumed to be involved in detection actually diminished, while awareness gained because many tools included awareness features along with those for prevention and so forth. The feature role categorizations are likely more accurate than the solution role categorizations because the features were categorized after more was known about the item being analyzed.

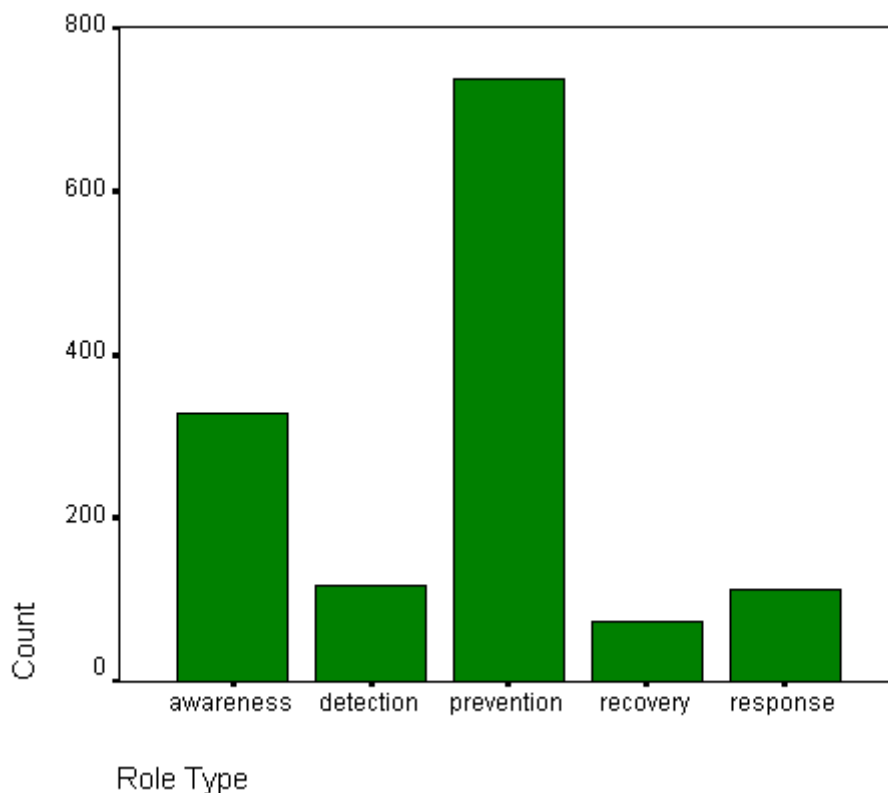


Figure 12: Feature Roles



Discussion

The emphasis on online privacy in the media led to a steep rise in availability of privacy solutions in the late 1990s and in 2000. The dot-com crash and events of September 11, 2001 seem to have led to a decline in interest in privacy and in producing privacy products. However, 2002 is off to a pretty good start (even though the information for the year is incomplete).

In terms of who is producing for the privacy space, it looks like there is a heavy contribution from lone entrepreneurs (Figures 2 and 3), working on very specific solutions (Figure 9), using commonplace interface technology (Figure 10), in hopes of making money (Figure 4), by targeting the most common operating systems (Figure 5). Unfortunately, the consumer market (Figure 6) may not be as good as they had hoped. However, many of these solutions have been adopted by larger companies who produce privacy software suites (e.g. Norton Internet Security 2002, Microsoft adding ever more built-in privacy features to Internet Explorer and the Windows operating system). Most of the solutions evaluated in the study are still available today, so there must be some demand for the features that they offer, especially those that prevent potential problems. There is still much work to be done in the areas of detection, response and recovery.


Privacy tools and services clearly have a market, but that market appears to be smaller

and less profitable than many had anticipated. A few of the tools, such as personal firewalls and virus scanners, have gained traction. Others, especially encryption products, are slowly finding their niches. Companies are re-targeting their products for enterprise applications or for use by network and system administrators, which has historically been a more reliable market for tools and services that are preventative in nature.

There are many trade-offs to consider when selecting privacy solutions. They are difficult to configure, and can interfere with a computer's expected functionality and some have a steep learning curve. End users will have no patience with software that interferes with the tasks they are trying to complete if they can see no benefit to using it. Privacy software is unusual in that when it works successfully, unexpected intrusions or other problems are averted and appear to not have existed at all. The problem is obvious; you can't prove a negative. User feedback such as graphical meters, pop-up messages, or logging mechanisms at least give people something to look at to see if their expectations are being met. More of these kinds of awareness-raising features are needed, but at the same time, it is important not to overwhelm users with too much information or distract them from what they are working on unless absolutely necessary.



Conclusion

The next phase of this research is to analyze the features more closely and work on validating the role categories. A major goal of this study is to build a framework for describing the privacy space. Once that framework is established, solutions can be categorized according to their features. The framework will form the basis for a system that will allow people to encode their online privacy expectations and then receive recommendations about which tools and services are required to instantiate those expectations. Once an online privacy posture is invoked, the framework will also be useful in testing if it is meeting those expectations as they change over time. 

About the Author

Benjamin Brunk is a doctoral student in the School of Information and Library Science at the University of North Carolina at Chapel Hill and manages the Interaction Design Laboratory (<http://ils.unc.edu/idl>) for Dr. Gary Marchionini (his adviser). This research was conducted during the first half of his dissertation entitled "A Framework for Understanding the Privacy Space."

Web: <http://ils.unc.edu/~brunkb>

E-mail: brunkb@ils.unc.edu

Acknowledgments

The author would like to thank the School of Information and Library Science at the University of North Carolina at Chapel Hill for its financial support, Dr. Gary Marchionini for his editing and advice, and his dissertation committee (Dr. Barbara

Wildemuth, Dr. Gregory Newby, Mr. Paul Jones, and Dr. Julie Earp) as well as Meg Nystrom for helping him with this work.

Notes

1. Refer to the definition of privacy discussed in the privacy subsection of the Introduction.
2. "Significant use of graphics" means that the feature included some graphic element beyond the everyday GUI - some kind of special visualization of pertinent information such as an animation, gauge, or meter.
3. Although one that is being eclipsed by GPG, the GNU open source alternative.

References

E.P. Bucy, A. Lang, R.F. Potter, and M.E. Grabe, 1999. "Formal features of cyberspace: Relationships between Web page complexity and site traffic," *Journal of the American Society of Information Science*, volume 50, number 13, pp. 1246-1256.

T.M. Cooley, 1888. *A Treatise on the Law of Torts*. Second edition. Chicago: Callaghan.

D.H. Flaherty, 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: University of North Carolina Press.

B. Friedman and P.H. Kahn, Jr., 2002. "Human values, ethics, and design," In: J.A. Jacko and A. Sears (editors). *The Human-computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*. Mahwah, N.J.: Lawrence Erlbaum.

B.G. Glaser and A.L. Strauss, 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine.

S.W. Haas and E.S. Grams, 2000. "Readers, authors and page structure: A Discussion of four questions arising from a content analysis of Web pages," *Journal of the American Society of Information Science*, volume 51, number 2, pp. 181-192.

D.L. Hoffman, T.P. Novak, and A. Schlosser, 2000. "Consumer Control in Online Environments," Working Paper, Vanderbilt University at <http://advertising.utexas.edu/vcbg/home/Hoffman00.pdf>, accessed 20 September 2002.

B. Schneier, 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley.

F.D. Schoeman (editor), 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

R.P. Weber, 1990. *Basic Content Analysis*. Second edition. Newbury Park, Calif.: Sage.

Editorial history

Paper received 22 August 2002; accepted 19 September 2002.

[Contents](#) [Index](#)

Copyright ©2002, First Monday

Copyright ©2002, Benjamin D. Brunk

Understanding the Privacy Space by Benjamin D. Brunk
First Monday, volume 7, number 10 (October 2002),
URL: http://firstmonday.org/issues/issue7_10/brunk/index.html