Members of the University may send comment on this report to the facilitators of the Task Force, Dave Millar—millar@pobox.upenn.edu — or Ira Winston—ira@central.cis.upenn.edu. The complete membership is listed on the fourth page of the report.

Final Report of the Electronic Privacy Task Force *June, 1994*

I. Summary and Recommendations

The Electronic Privacy Task Force was convened jointly by Dr. Peter Patton, Vice Provost for Information Systems and Computing, and by the University Council Committee on Communications, with the following objectives:

- To identify and articulate the electronic privacy issues facing Penn.
- To develop options for resolving these issues.
- To recommend solutions to them.

The purpose was not to write a privacy policy, but to build a consensus on what the issues are, and how they should be resolved. The Task Force considered a range of solutions including creating new policies, or modifying existing ones, as well as efforts to increase awareness of the problem. This report is intended to guide the creation of University policy, consistent with other applicable policies, under the aegis of the Communications Committee.

In particular, the group was charged with defining the obligations of the University to respect and protect the privacy of the individual. The University policy on "Ethical Behavior with Respect to the Electronic Environment" addresses the threat to privacy that a malicious individual poses. It does not, however, address the accidental or intentional disclosure of confidential information by individuals responsible for managing systems in the course of their duties.

The purpose of this report is two-fold. One is to communicate to the Penn community the recommendations of the Task Force with enough force to ensure that progress continues. This report is only a first step towards resolving the problems of electronic privacy.

The second, and equally important purpose, is to increase the awareness of all members of the community of the issues of electronic privacy. The members of the task force felt that one of the biggest problems was a lack of knowledge and understanding. It is hoped that this document will make people think about how the problem of electronic privacy affects them and will motivate them to support efforts to resolve the problems.

While privacy is an important issue to many individuals at Penn, it is just as important an issue to the University as a whole. The U.S. legal system is straining to keep up with the new dilemmas wrought by advances in technology. Courts are only now *beginning* to try to clarify the issue of employee privacy in light of electronic communications technology. Without clear statutes and precedents as guidance, an employer lacking clear privacy policies and standards risks running afoul of the law through the actions of malicious or even well-meaning, but misinformed employees.

The Issues of Electronic Privacy

The Task Force developed the following statement of the issues of electronic privacy:

1. Who owns information?
2. What are the rights to privacy of data, specifically including data created and controlled by individuals, and data about people?
3. Who has responsibility for protecting privacy rights?
4. People do not know what data are kept about them, including data intentionally kept about them (e.g., personnel records, medical history, salary history, etc.) as well as data incidentally kept about them (logs of access to buildings, logs of access to networks, systems).
5. People do not know that there are such things as illegal files and unacceptable files.
6. System administrators sometimes use data for purposes other than those intended when they were collected.
7. There is no clearly-defined process for authorizing system administrators to release information, or to conduct monitoring as part of an investigation.
8. System administrators often believe that their duties do not include assisting legitimate, authorized investigations.
9. System administrators do not know the extent of their responsibility to protect their systems from illegal files (child pornography, pirated software), or potentially harmful files (password-cracking software, viruses, etc.).
10. Conducting a computer investigation requires specialized skills, which only a few groups and individuals on campus possess.

Recommendations

To address the above issues, the task force makes the following recommendations:

A. For major categories of personally-identifiable electronic data, a set of privacy policies should be adopted by the University. If any group responsible for the management of a computer system feels that any of the policies are inappropriate for their computer system, they may write their own privacy policy, but must publicize the policy.

Policies should be created for the following categories of data: electronic mail, voice mail, University administrative data, and University academic data. A policy should also be created for campus computer networks which carry a mixture of all categories of data.

Policies should distinguish between the treatment of data about or created by students, faculty and staff if a legal, or other sound basis exists.

Before a new policy is created, consideration should be given to reinterpreting or amending existing policy to address the issue of electronic privacy.

The creation of privacy policies (both those drafted for University-wide applicability and those targeted where University-wide policy is inappropriate) should be guided by these principles:

1. Where appropriate, policy should be guided by expectations of privacy in more traditional, non-electronic domains. For data stored on one's desktop computer, or for data stored in a personal account on a multi-user system, a good analogy is that the privacy afforded such data should be the same as the privacy afforded the contents of one's desk, office, lab or dorm room.
2. The office analogy is inappropriate for data that the University holds about individuals. For such data, the following principles should guide policy creation:
   a. Subjects of data should know the purpose for which data are collected.
   b. Subjects should be informed of any new uses of data beyond the original, stated purpose.
   c. Guidelines should define what data are kept about people.
   d. Guidelines should define how people may inspect and correct data.
   e. Only data necessary for a particular purpose should be collected.
   f. Personally-identifiable data should be disposed of where possible.
   g. The accuracy, reliability, completeness, and timeliness of data should be ensured.

Finally, for all categories of data, the following principles should guide the creation of policy:

a. Guidelines should define under what circumstances data will be released.
b. Guidelines should define who has access to data.
c. Guidelines should define how data are safeguarded from unauthorized access.

B. A set of electronic privacy guidelines should be created for anyone with systems administration duties. These guidelines should be included in campus systems administrators' job descriptions, and should be communicated to all new and existing employees with system administration responsibilities. Such guidelines should address both proactive steps to be taken to increase privacy, as well as restrictions over activities which may decrease privacy.

C. Awareness of the issues of electronic privacy should be increased. Specifically, the Vice Provost for Information Systems and Computing should inform the general Penn community of electronic privacy issues through articles, training sessions, and by facilitating campus-wide discussion of the issues. Additionally, electronic privacy should be included as a topic during "Penn Perspective," "Penn Supervisor," and other appropriate Organizational Development and Training classes. Finally, it is necessary that any individuals with access to confidential records understand that the records are private and that violation of that privacy could lead to disciplinary action.

D. The Office of the Vice Provost for Information Systems and Computing should work to increase awareness and acceptance of electronic privacy standards.

(continued next page)

E. The Statement of Stewardship of Human and Financial Resources should be expanded to cover issues of electronic privacy.

F. In one year, a review of progress in addressing the issues of electronic privacy should be conducted.

II. Why worry about electronic privacy?

"The most important computer privacy problem facing Penn today is the general level of ignorance about how much information is being gathered and stored, and about the myriad ways in which this information can be used to limit, direct, or otherwise influence ... one's experience at the University."

— Professor Oscar H. Gandy
The Annenberg School for Communication

People sometimes wonder why they should worry about electronic privacy. Many people have never been harmed by a violation of their privacy, and they do not know anyone who has. So what is the problem? What are the risks? What are the threats?

Consider the following incidents:

1. Twice in three years, a Penn faculty member had a fraudulent credit card established in his name. His credit record showed large, unpaid bills to the credit card company. How was the credit card obtained? Someone was able to provide the issuing bank with a correct address and social security number. Without the social security number, the credit card would not have been issued.

2. A Penn student wrote a computer program which checked to see what computers a person is logged in from. The program kept a record of the physical movements of anyone using campus computers.

3. A Philadelphia-area journalist, investigating underground computer hackers, attended a "hacker's conference" at a local hotel. At the conference, she was presented with a copy of her credit report, with a warning that if she continued to investigate, her credit report would be altered.

4. In February, 1994, the following announcement appeared on Internet news groups:

> "Infotech is an Information Provider and we have recently begun providing our services via the Internet. A partial list of some of our services include:
>
> Individual Credit Reports * Business Credit Reports * Dun & Bradstreet * Pre-Tenant Background Check * SS# Locator Service * National Change of Addr * Difficult Phone Numbers * Nationwide Marriage, Divorce and Death Records * Criminal Records Search * Arrest & Convictions Records * Bank Acct Search * Real Property Search * Workers Comp Claims * Consumer Affairs Reports * Corporation Search * Tax Lien Search * Corp. Bankruptcy Search * Business Name Search * DMV Records * Registered Voter Search * Nationwide Warrants* And MUCH MORE!"

In a survey of over 300 U.S. businesses, a report in the June, 1993 issue of *Macworld* found that more than 21 percent of those polled said they had "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications." "Monitoring work flow" was the most frequently cited reason for electronic searches.

The threats to privacy have grown in recent years for a number of reasons. For one thing, more data about us is stored on computers. Much of that data, we are not even aware of. For another thing, the computers storing this data are more likely to be connected to a network today. That means that it is not necessary for someone to gain physical access to a computer to view confidential information. If a computer is connected to the Internet (as are virtually all computers at Penn) it is accessible literally from anywhere in the world. As if matters were not bad enough, the nature of electronic media make it quite difficult to even know when our privacy has been violated. And finally, very often, the data that we think is probably the most private—that which we create and store in our own private files—may not be as private as we think.

The data that is stored about us is often invisible to us. Sometimes people do not stop to think that when they log into a computer, or when they swipe an access card to enter a building, they are creating an electronic "footprint" of where they go, and how they spend their time. It may not occur to someone that it is possible that records are kept of what electronic news groups they read, or how much time they spend reading them. It may not occur to someone that another person may be able to see what newsgroup they are reading *at that very moment*. People may not be aware that electronic messages, which they thought they had deleted, are in fact stored on a backup copy somewhere. In some cases, we may be aware that data are kept about us for one purpose, but we might be surprised to find out who they were subsequently given to for quite a different purpose.

People sometimes think "I have a clean conscience. I've done nothing wrong. The only people who need to worry about privacy are people who have something to hide." That might be true if one could be certain that every piece of personal data was completely accurate. But even if it were possible to discover every instance of personal information, is one able to verify it and correct all inaccuracies? That is the problem that the Penn professor above faced after his credit record had been ruined.

During the last two decades there has been a significant change in our "private space." Twenty years ago we were assigned office space, lab space or dorm rooms. Within that space we were able to provide security for private information by locking desks and file cabinets. We were comfortable because we had a high degree of control over our private information, and because we felt that our expectation of privacy was consistent with the privacy that we were afforded. In fact, most of us hardly gave privacy a second thought: there was little reason to fear its loss.

Today, our physical office is only a part of our "virtual office." Our virtual office includes electronic information located on computers outside of our physical office. This information includes research data, electronic mail, and voice mail, and is stored on numerous different computers. Throughout the University, hundreds of such computers are managed by a variety of employees, many of whom are aware of their ethical and legal obligations to honor privacy rights. Nevertheless, over the past few years there have been instances of questionable searches and monitoring of electronic information. So it is difficult to be sure that even our most private data—that which we create ourselves—remains private.

Today we have less control over the privacy of our information, and many of us are not at all certain that the degree of privacy that we desire is consistent with the privacy we can expect. In fact, it is difficult to get factual information about how much privacy we can expect.

Our concern is that privacy rights, which we once rarely gave a second thought, will now be lost in the rapidly developing world of electronic technology. This concern is based on the potential for abuse of privacy through electronic means.

The greater potential for abuse of privacy in electronic media stems from the discreet manner in which information can be collected. With our private and personal information spread out over dozens or hundreds of physically separate computers, it is quite possible for private information about us to be disclosed without our knowledge. Electronic burglars, if they are any good, rarely leave behind obvious evidence of their intrusion.

In the past, we could comfort ourselves with the thought that confidential information about us was distributed across so many different computers, that any disclosure of private information would at least be limited in scope. The thought that all or much of the electronic information about us could be somehow assembled into a consistent whole did not seem plausible. However, as computers are increasingly linked together through networks, the threat becomes more plausible, as noted in item four above.

In summary, it is rational to be concerned about privacy for several reasons:

- Increasingly, data are kept about us without our knowledge.
- Lacking knowledge about what data are kept about us, it is impossible to know whether the data are accurate, and whether decisions being made based on them are proper.
- Increasingly, we keep our own data in places where we can not be certain that they will remain private.

Clearly, we need better information about what data are kept about us, how they are protected from unauthorized disclosure, and what our rights to privacy are.

III. Legal Status

Two federal laws pertain to privacy at Penn: the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Electronic Communications and Privacy Act of 1986 (ECPA).

FERPA (Buckley Amendment)

FERPA is designed to protect the privacy of a student's educational records. Students have the right to inspect and review all of their records maintained by the school. Students have the right to request that a school correct inaccurate or misleading records. The school must have written permission from the student before releasing any information. However, the law allows schools to disclose records, without consent, to school employees who have a need to know, and other individuals or organizations in certain defined circumstances.

Schools are permitted to release directory information, unless the student objects. Directory information includes, for example, name, address, telephone number, date and place of birth, and other biographical information.

E-mail addresses would likely be considered directory information.

Schools are required to give public notice of

- What is considered directory information
- A student's right to refuse release of directory information
- The time period for the student to refuse release of information.

ECPA

The ECPA outlaws unauthorized access to electronic communications. This only applies to electronic communication services being provided to the public. It appears that Penn is not considered an electronic communication service provider as defined in the law, though some have argued that our student e-mail systems are covered by the law.

No cases have come to any District Courts testing the act. The best guidance is to look at how courts have handled cases of telephone monitoring. Courts generally frown on employers' routine monitoring absent suspicion of wrongdoing, or where the employee has been given reason to believe that phone conversations will not be monitored.

Cases have generally hinged on an employee's "reasonable expectation of privacy." A reasonable expectation of privacy is not an absolute standard. In fact, it is quite the opposite. An employer can influence an employee's reasonable expectation of privacy by informing employees what types of monitoring they are subject to. Employers are generally allowed considerable latitude in monitoring, as long as employees are made aware of the monitoring. Any monitoring by an employer without prior notice, is more likely to be considered a violation of an employee's reasonable expectation. Therefore, it is in the employer's interest to clearly state in advance the circumstances and the types of monitoring that may occur.

We are probably within our rights in electronic monitoring when we have specific knowledge of potential or actual harm to our networks or computers, and where the monitoring is narrow in scope. We need to be careful when the information monitored may be used for other purposes, such as disciplinary proceedings or criminal investigations.

When other organizations tell us that attacks on their computers are coming from Penn, we should require a written statement from the institution stating the specifics of what harm was done or attempted.

IV. Analysis of the Issues of Electronic Privacy

In the course of debating and discussing the issues of electronic privacy, the Task Force found it necessary to agree to differ on some of the issues. While some common ground was found, and many insights were discovered during the discussions, the group found that consensus was not always possible.

It was felt that there was value to including in this final report a summary of how the Task Force approached the issues of electronic privacy, whether or not complete consensus was reached. This section summarizes how the Task Force analyzed the information gathered, how the group reached the conclusions included in the final recommendations, and where opinions were divided.

How Much Privacy to Guarantee

Whereas there was broad agreement among the Task Force on the need for a concise "expectation of privacy" statement, there was little consensus on how much privacy to guarantee. These comments from members of the Task Force reflect the broad range of opinions held:

"The right of the individual to determine if, when, and how information about them will be collected and used is fundamental."

"If I, as a supervisor, suspect that an employee is wasting time on the computer, then I should be allowed to see logs of how they're spending their time."

The Task Force noted that whatever rights to privacy are promised, the University may not be capable of preventing violation of those rights. Some Task Force members concluded from this that it is better to guarantee less privacy than to offer broad privacy rights which we may not be capable of enforcing.

Is everyone entitled to the same degree of privacy?

It appears that from a *legal* standpoint, students, prospective students, alumni, faculty and staff may have differing privacy rights. As noted in Section III, Legal Status, courts have found that employers may monitor employees' communications when the employer provides advance notification. Staff, as employees of the University, may, therefore have only limited *legal* privacy rights. Given the special role of faculty, they may have stronger legal claims to privacy than staff. Student records have specific legal protection provided by the Family Educational Rights and Privacy Act (Buckley Amendment). Alumni, as former students, would likely have privacy rights analogous to those of students, at least concerning the alumnus' student records. Prospective students, while not covered explicitly under the Buckley Amendment, are granted certain privacy rights in Penn policy.

While the above addresses the question of a *legal* right to privacy, it begs the ethical aspect of the question. Some members of the Task Force felt that as an institution of higher learning which values free speech, Penn should establish a higher standard of privacy than the minimum required by law.

Due Process for Investigations

"All requests for exceptions to a strict privacy shield, whether internal, or external to the University should be held to the highest level of evidence"

—Professor Oscar Gandy

"Penn should not constrain itself with any procedural obstacles to conducting investigations. Subjects of investigations, and their lawyers, will only use such procedures, and our failure to follow them precisely, as a way to cloak themselves from prosecution. Furthermore, we will take away the flexibility that we need by spelling out, in advance, an investigative process. There is no way for us to foresee the kinds of incidents which might come up, and the ways in which such a process might be subverted"

—Associate General Counsel Neil Hamburg

The Task Force generally agreed that there were situations in which otherwise private information may need to be disclosed. One example is when there is strong evidence of a possible violation of laws or University policies.

The Task Force was divided on whether or not a formal process was required to authorize the release of such data.

When served with a subpoena or search warrant from a law enforcement agency, Penn has little recourse.

The Task Force agreed that, in the course of an internal University investigation, some form of approval by an independent and objective third party should be given before confidential information is released. A majority of the Task Force felt that such a process should be formalized. The Task Force was not unanimous on this issue, however. The Task Force agreed that there should at least be informal procedures for approving investigations seeking access to private data.

Some members preferred that additional protections of due process be made part of a formal procedure for authorizing investigations.

What kind of data does this report address?

The issue of electronic privacy is potentially quite broad in scope, and may pertain to many different types of data:

- Data stored on personal computers
- Data stored on multi-user computers
- Logs of system or network access
- Voice mail messages
- Logs of building access
- Data in-transit on the network
- Backup tapes, system archives

The data pertinent to electronic privacy is personally-identifiable data concerning Penn faculty, students, prospective students, alumni, or staff. Data not about such individuals, and data which has been summarized in such a way as to eliminate any personally-identifiable information, are not addressed in this report, as they do not pose a threat to the electronic privacy of members of the Penn community.

However, Professor Gandy notes that personally-identifiable data is not the end of the road with respect to electronic privacy:

"Our concerns regarding privacy have to do with consequences that flow from [the use of information]. Individuals may be discriminated against ... on the basis of personal information. Frequently that discrimination is based on their identification as members of [either] a "real" group, as generally recognized (race, gender, school, etc..) or more transitory putative groups (high risk, multiple offenders, dishonest, etc.). To the degree that data are used to make assessments about groups, to which individuals may be assigned, and share the treatment of the group, there are group privacy concerns. Thus, data summarized, are frequently used to make decisions about groups ... in which there are individuals who suffer the consequences of classification and misclassification."

Guidelines for those with System Administration Duties

When someone with system administration duties receives a request for private information, the administrator is often reluctant to honor the request for fear of incurring legal liability both personal, and of the University. However, it is sometimes difficult to identify and refuse improper requests without privacy guidelines in place.

At the same time, some members of the Task Force had first-hand experience with system administrators who were less conscious of their legal

and ethical privacy obligations.

Generally, it was agreed that those with system administration duties should be allowed to view all data on the system they manage, including private files, when investigating documented problems of system integrity or responsiveness. As a control over such wide-ranging power, however, all such information should be kept confidential, except where such information contains evidence of a violation of laws or University policy. People who view private information must behave as if they had not seen the information.

The Task Force concluded that a set of guidelines for those with system administration duties are required to clarify issues of electronic privacy.

Policy or Principles

The Task Force had to determine how best to ensure appropriate levels of privacy for systems and data at Penn.

It is not the role of the Task Force to develop a University-wide privacy policy, but to *identify the issues* of electronic privacy, and to *propose principles* addressing those issues. The Task Force felt that this could be best accomplished by directing the process of extending existing policies to the electronic environment and by identifying areas where privacy policies do not exist and should. The issue of electronic privacy is quite broad in scope, limited not only to administrative computer systems, but extending into areas such as research data, voice mail systems, and campus debit cards. The rapid pace of technological change is likely to present more challenging problems. The group felt that it would be difficult, if not impossible, to write a comprehensive, University-wide electronic privacy policy which adequately covered all aspects of the problem in all possible situations.

At the same time, the Task Force was mindful of the need for a degree of consistency in the privacy afforded electronic data across the many departments, units and centers of the University. It is futile for one system to enforce strict privacy provisions if that system communicates to, and shares data with, other campus systems on which privacy is not respected.

The Task Force proposed that for major categories of personally-identifiable electronic data, a set of privacy policies should be adopted by the University. If any group responsible for the management of a computer system feels that any of the policies are inappropriate for their computer system, they may write their own privacy policy, but must publicize the policy. All such policies should be consistent with the principles that are outlined in Section 1.

Is Privacy any Different for Computers?

"*Computer privacy is not much different than privacy in other forums. If the University has a right to look in a student's dorm room, then they should have a right to look at the student's computer account. However, there are several differences:*

1. It is easier for the subject to learn of a physical search than a computer search.

2. Physical searches are more difficult to conduct."

— Dr. Al Shar, School of Medicine

"As for the important difference between computers and the other sections of the office, I can't delete my office, my officemate's appointment calendar, or the work that we've been doing for the past ten years without a large incendiary device. I can do these things by giving out my password, having any half competent hacker tell me how, and FT-Ping the entire company technical database in a little over 20 minutes anywhere in the world."

— Penn staff employee (taken from upenn.talk)

The Task Force concluded that in many ways, the issues of electronic privacy are not much different than more traditional privacy issues. In fact, it often served the group well to analyze issues of electronic privacy by searching for analogs from other fields. The significant difference, however, is the capacity that technology affords for widespread abuse of privacy in the electronic forum.

Because most of the issues of electronic privacy are not unique, it may be possible to find guidance in Penn policies which deal generally with the issue of privacy.

In some cases, the policies which deal with privacy were written without considering the issue of electronic privacy. The Task Force urges that, wherever possible, such policies be amended, revised or reinterpreted to consider information and communications technology.

Task Force Membership and Approach

Members serving on the Task Force included:

Steven Blum, Director, Student Dispute Resolution Center, and Judicial Inquiry Officer
Prof. David Farber, Alfred Fitler Moore Professor of Telecommunication Systems, SEAS
Prof. Oscar Gandy, Annenberg School
Neil Hamburg, Associate General Counsel
John Kuprevich, Commissioner, Public Safety
Dave Millar, University Information Security Officer
Prof. Gerald Porter, SAS, Past Chair of the Faculty Senate
Prof. Martin Pring, Medical School
Dr. Albert Shar, Medical School
Chris Shull, Open Systems Specialist, Information Systems & Computing
Rob Terrell, Assistant General Counsel
Gary Truhlar, Director, Human Resources Information Management
Daniel Updegrove, Associate Vice Provost, Information Systems & Computing
Mr. Ira Winston, Director, SEAS Computing

The Task Force was jointly led and facilitated by Ira Winston and Dave Millar.

The Task Force met seven times between November, 1993 and March, 1994. During that time, the group:

- Worked to define the issues of electronic privacy at Penn.
- Heard from a variety of campus representatives including students, faculty and staff about their perception of the issues of electronic privacy.
- Surveyed what other institutions have done about electronic privacy.
- Reviewed Penn policies pertaining to privacy.
- Reviewed Federal and state statutes and case law pertaining to privacy.
- Developed recommendations to remedy the issues discovered.

Appendix—What Others Have Done

The Task Force reviewed what other institutions (academic and others) have done about electronic privacy. What follows is a brief summary of the policies reviewed.

The policies generally fell into one of three categories:

Strong Privacy Protections: Two of the eight institutions surveyed had policies that fell into this category. These policies had the following provisions: : :

"All computer users are entitled to broad privacy rights."

"Information will only be disclosed with approval from university officials."

"Where appropriate, users will receive prior notice of such disclosures."

Moderate Privacy Protections: The five institutions in this category included the following provisions:

"Managers and supervisors can, in some circumstances, create and limit the expectation of privacy by letting people know who has access to which data and for what purposes."

"Administrators will try to honor student's rights to privacy."

"Electronic mail ... is as private as we can make it."

Weak Privacy Protections: This institution had a policy which included the following provision:

"The University reserves the rights to inspect, copy, remove or otherwise alter any data, file, or system resources which may undermine the authorized use of that system, with or without prior notice to the user.

"The University shall not be liable for, and the user assumes the risk of, loss of data or interference with files resulting from the University's efforts to maintain the privacy and security of the University's computer, information and network facilities."

The one policy which the Task Force generally agreed best represented their views was that of Colby College, which is excerpted here:

"Personal electronic information (e-mail, files, etc.) are considered within the same context as an individual's student room or faculty office. The College does not search those personal areas without appropriate authorization and that authorization cannot come from within Computer Services. The rights to privacy and due process must be observed."

"Restrictions on access to files in a staff member's account are less severe because the account is used in carrying out the individual's job. In the event of absence, material related to that job may be needed by others and it is assumed that the supervisor or department chair may authorize access. In the event of suspected misconduct, care would be taken to obtain authorization to explore files."

"Computer Service organizations need to avoid being investigator, prosecutor, judge, jury, and executioner. Sometimes we are too close to the situation to be objective, though."