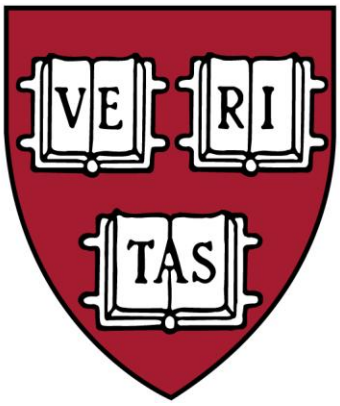
HARVARD UNIVERSITY



REPORT OF THE ELECTRONIC COMMUNICATIONS POLICY TASK FORCE

FEBRUARY 2014

Introduction

The Harvard University Task Force on Electronic Communications Policy began its work last spring, following a controversy over a decision by University officials to access certain electronic information through the University's information systems. The controversy revealed that University policies regarding access to such information were neither clear nor well known. The controversy also brought to the fore a range of issues that needed more systematic consideration. In response, President Faust established this Task Force.[1]

In her charge, President Faust directed the Task Force to "consider and recommend appropriate policies regarding access to, and confidentiality of, electronic communications that rely on University information systems." President Faust further instructed the Task Force "to focus on recommending policies for the future that are both principled and practicable and that account for the reasonable expectations of individuals, the legitimate interests of the University, and associated issues of notice and process." The charge made clear that the Task Force was "not expected to investigate or render judgments on past events," as Michael Keating, a lawyer at the Boston law firm of Foley Hoag, had been asked to examine the specific actions that gave rise to the controversy last spring. But President Faust did instruct the Task Force "to take general account of instructive examples at Harvard and elsewhere as one means to understand the complexity of considerations that can inform sound recommendations for the future." President Faust also requested that the Task Force "consider whether and to what extent Harvard's policies should be University-wide or specific to certain parts of the University or particular institutional roles and responsibilities," and she requested that the Task Force "consult widely" with the University community and inform itself of "best practices" at the University and elsewhere[2]

The Task Force met roughly a dozen times over the spring and the fall. At those meetings, we sought to identify critical issues, work through possible scenarios, and formulate solutions. In addition to these discussions, the Task Force reached out to a wide range of people both inside the University community and beyond.

Specifically, the Task Force met with student leaders from the Undergraduate Council, which provided an online survey of undergraduate views about the issue, and the Harvard Graduate Council, which provided a summary of responses to a survey of its members. The Task Force, in whole or in part, also met with a number of individual faculty, staff, and administrators, as well as with Michael Keating, who briefed the Task Force on the findings set forth in the report that he completed last summer. Members of the Task Force also met with the

[1] The Task Force is composed of 16 members and includes faculty and administrators from each of the University's graduate Schools, as well as from the Faculty of Arts and Sciences. The vice president and general counsel, the vice president and University chief information officer, the vice president for human resources, and the vice president for strategy and programs were also assigned to the Task Force. Two of the original members of the Task Force left the University for other employment before our work concluded. A document setting forth the membership of the Task Force appears as Appendix A to this report.

[2] The charge to the Task Force appears as Appendix B to this report.

deans and faculties of numerous Schools within the University, either at regular faculty meetings or faculty committee meetings, or both, and the Task Force received comments from two University-wide open forums that it hosted as well as from an electronic community discussion board that it established. In addition, the Task Force met with the Council of Deans, the Board of Overseers Committee on Institutional Policy, and the Harvard Corporation. The Task Force also reached out to peer institutions to learn from their experiences and policies in this area, and it did considerable reading about the trade-offs complex institutions face in grappling with issues in this area. In all, the Task Force met, individually or in groups, with about 500 members of the University community.

This report sets out and explains the Task Force's recommendations. Consistent with President Faust's charge, they are the product of extensive discussion within the Task Force itself, and they have benefited greatly from input received from all parts of the University community.

The Task Force recommends the University adopt a comprehensive policy regarding access to electronic information that would apply across all components, faculties, and Schools. At present, the University lacks a clear, overarching policy in this area. The absence of a single, visible, and comprehensive policy has led to confusion and uncertainty. Most troubling, it has led some to distrust the process for deciding how and when access to information transmitted over, or stored on, University systems, networks, and devices may be undertaken. A single policy will best ensure the University makes decisions regarding access pursuant to rules and processes that are established in advance and known to the community as a whole. In addition, a single, comprehensive policy will mitigate the hazards of ad hoc decision-making under intense time pressure that otherwise may be expected to arise.

This report also explains what the Task Force recommends for inclusion in a University policy. Its recommendations aim to honor the University's commitment to academic freedom and free inquiry while being sensitive to the University's administrative and operational needs. The Task Force believes the implementation of its recommendations can accomplish this goal. It is the Task Force's view that the recommended policy would instill greater confidence and trust within the University, including in those limited circumstances when access may be legitimately authorized.

The key to formulating such a policy, in the Task Force's view, lies in establishing processes and structures that ensure any decision to authorize access is made (1) in an accountable and transparent fashion, (2) pursuant to advance guidance about when such authorization is legitimate, (3) on terms that ensure that access will be carried out only through narrow means and with suitable checks against unwarranted disclosures or intrusions, and (4) subject to periodic oversight by a committee that includes faculty representation. Some of the recommendations that follow formalize University practices that are already in place but that have not been clearly codified. Others codify policies that had not been consistently

implemented. Still others reflect the judgment that additional safeguards and protocols should be implemented. In brief form, the key features of the proposed policy are:

- **Limited Justifications for Access:** Acess to electronic information should be permitted only for a legitimate and important University purpose, as informed by the illustrative list of the limited purposes that have historically justified such access.

- **High-Level, Accountable Authorization:** In general, access to electronic information for reasons other than systems maintenance and protection should be undertaken by information technology personnel only when specifically authorized by the head of the School or component of the University making the request, such as a dean of a faculty.

- **Notice to Users:** There should be a strong presumption that users should receive timely notice in any case in which access to their electronic information has been authorized.

- **Minimization Rules and Protocols:** Access to electronic information, if authorized, should be undertaken in a narrow manner and pursuant to minimization rules and protocols that information technology components have codified in advance.

- **Record-Keeping:** Written records of decisions to access electronic information should be prepared in a manner that permits subsequent review of such decisions.

- **Independent Oversight Committee:** Decisions to authorize access to electronic information should be subject to periodic review by an oversight committee that includes faculty in order to ensure an independent set of "eyes" also lends its perspective on any such decisions and on possible policy or process changes.

In offering these recommendations, the Task Force recognizes the University maintains information networks, systems, and devices for the benefit of the community as a whole. The University's successful operation requires they function well. A policy must ensure these systems facilitate the University's broad range of activities and permit the University to meet its responsibilities. The Task Force also recognizes that electronic information has, in many respects, supplanted paper files as the chief mechanism for creating the records and communications of University operations—records and communications the University has long had a legitimate interest in accessing in appropriate circumstances and by appropriate means. For that reason, those who use these networks, systems, and devices should be aware of the University's legitimate interests in obtaining access to electronic information in certain circumstances—and also of the important limitations and safeguards concerning how and when access may be authorized and carried out. Such awareness helps members of the University

community to make informed and prudent judgments in using this distinct means of communication.

As important as the Task Force believes these recommendations are, it is hard to foresee what may turn out to be the most challenging issues due to the rapidly changing nature of technology and the great variety of University operations. For that reason, the Task Force also recommends the University establish a mechanism, perhaps involving the Task Force's proposed oversight committee, to enable faculty to work with the administration in proactively considering the range of issues related to electronic information privacy that are likely to arise.

The shift in the technological means by which we communicate with one another yields great benefits. It also presents new challenges and trade-offs. This shift in technology should not, however, fundamentally change the nature of the University community. It is a special place for teaching and learning, and it is a place in which a sense of mutual trust is vital. The Task Force offers its recommendations in the belief that the proposed safeguards will help ensure that the greater access to electronic information that is now possible does not subtly erode longstanding expectations about the University's relationship to those who work, teach, and learn here.

The report proceeds as follows. It first identifies and further defines the nature of the problem the Task Force's recommendations address. It then identifies the principles that animate the Task Force's analysis of that problem. The report next works through the trade-offs that, in light of these principles, must be resolved at each stage of a potential decision to permit access to electronic information, and, along the way, offers recommendations that pertain to each stage of the decision-making process. The report concludes with a recommendation about how the University should position itself to address and anticipate related privacy issues in the future. The Task Force has also drafted a "postable" policy that distills the report's recommendations in a form that can be communicated to users within the University community.

I. Nature of the Problem

Harvard, like all large organizations, has the technical capacity to access a great deal of information that is transmitted, stored, and communicated electronically by members of its community over systems, networks, and devices that it owns, provides, and/or manages. That capability inheres in administration of such systems and is necessary to their successful operation. But that capability also raises the possibility that the University, like any administrator of an information system, could access information traveling through, or stored on it, without the specific consent or knowledge of the system's users.

In practice, as we describe further below, the University has used this capacity in the vast majority of instances for purposes directly related to the maintenance and protection of the systems themselves, or to ensure the continuity of business operations in the event a staff

employee departs or is otherwise unavailable and critical administrative files need to be examined. These standard forms of access have not been a source of serious concern. But, as recent events show, other types of cases may raise significant concerns and require sensitive judgments. The University needs rules to ensure it makes such decisions in an accountable manner, consistent with the University's historic mission, and in keeping with its best traditions.

At present, Harvard does not have a clearly articulated policy—one that comprehensively regulates when such technical capacity may be relied upon to obtain access to electronic information that travels over, or is stored on, the systems, networks, and devices the University owns, provides, and/or administers. The fundamental problem the Task Force seeks to address arises from the absence of such a clear, University-wide policy. Therefore, our goal is to set forth as clearly as possible the rules, structures, and constraints that should govern decisions about whether and how to grant access, while also acknowledging when the exercise of sound and accountable discretion is necessary and appropriate.

Harvard is not unique in facing this problem. All large, complex institutions administer information technology systems that enable access to the electronic information members of their community generate. Many of these institutions, like Harvard, feel constrained, for reasons both practical and principled, to place limits on when and how they may access that information. From traditional commercial workplaces, to Internet services, such as Google and Facebook, to peer universities, there is a growing recognition of the sensitivity of electronic information—in part because networks capture user activities in ways previously unimaginable, and in part because the boundary between work and personal lives is blurring. Policies like the one our Task Force recommends reflect this felt need to exercise restraint in accessing electronic information stored on, or traveling over, information systems that large institutions want members of their community to use and that these institutions provide to facilitate their work.

Harvard's Technical Capacity

The University owns, provides, and/or administers various electronic systems, networks, and devices that students, faculty, and staff use. In addition, people outside the University community regularly communicate with members of the community through those same University networks, devices, and systems. To identify proper structures and constraints regarding access to the resulting electronic information, it is important to understand the technical capabilities of the University.

1. Email: Email is probably the most salient method of communications over these systems, networks, and devices. There are more than 14 major Harvard-owned or managed email systems serving more than 65,000 University-wide users that the University administers, either directly or through vendors. These systems, including MS Exchange, Harvard gmail, UNIX mail, and others, are both physically located on campus and in the cloud, and are managed by multiple groups across Harvard. Harvard's role in managing these email systems means the

University, like the administrator of any email system, has, at least in theory, the technical capacity to access these accounts without users being aware such access has occurred.

The University also has some capacity to access email accounts that it does not administer, though in very limited circumstances. This capacity is triggered when a user accesses such an account through a University network or when a user stores information from those accounts on servers the University owns or administers or on devices that it owns or administers. The University has the technical capacity to access only those portions of such accounts that travel across the network or that are stored on University-owned or University-managed systems and devices. Even then, the University has the capacity to obtain access only to such portions of the accounts and only during the limited time that those portions are traveling across the University network or that they are stored on systems or devices owned by the University.[3]

2. Information Other Than Email: The University's networks, systems, and devices also store and carry electronic information other than email. That information includes files, voice mail messages, records of library usage, texts, records of Web browsing, and swipe-card data. In sum, the University has the technical capacity to access electronic information through hardware (such as University-provided computers), storage systems (disks and backup files), communications (email, voice, video), or network packets (within Harvard and to the outside).

There is nothing surprising about this technical capacity, even though some members of the University community may be less aware of it than others. Nor is this capacity inherently problematic. Information systems must be managed and maintained in order to be useful to those who use them. That is true for ordinary businesses and commercial information services no less than for universities. Such management and maintenance can only occur if information technology administrators have access to the information stored on and traveling through these systems, networks, and devices. In fact, users regularly call upon University information technology staff to troubleshoot a computer problem or to recover a file that appears to have been lost. In seeking such help, users often rely on the access systems administrators have.

Because the University facilitates the generation of a wide range of electronic information, however, any policy governing access should apply to more than email. Sensitivities also apply to a wide range of user data, from academic or personal files stored on University-owned computers or devices, to records of Internet usage on Harvard accounts, to the contents of Web pages that travel over the University networks, to the so-called metadata that can disclose information about whom a person was communicating with and when. A policy that encompasses the full range of electronic information best ensures access decisions occur within a system of appropriate structures and constraints.

[3] Although the report makes reference to University-owned devices, in many instances the University will have no feasible means of obtaining access to them without at least the knowledge of the user because the University would have to physically obtain the device in the first instance.

Actual Practice

The abstract description of the University's technical capacity can be misleading. It is important to know the likelihood a user's information will be accessed in a manner that would implicate privacy interests. To get a more realistic sense of the University's access to electronic information, it is important to understand the different mechanisms for obtaining access that may be used and how they vary depending on the task at hand. In that regard, it is significant that only certain means of access likely raise substantial concerns and that the University takes steps to limit that kind of access. Further, in putting the potential for access in its proper context, it is important to remember that the University's technical ability to access electronic information does not mean that the University in fact accesses that information. For example, whatever its technical capabilities, the University does not engage in the practice of routinely monitoring user content. More specifically, the University has never intercepted for routine access packets that travel across its network in real time, nor does the University engage in full-packet capture across the network that would enable it to go back and look at, for example, non-Harvard email that travels across the network.

To further explain the relevant context, we set forth, as a historical matter, the limited circumstances in which access to electronic information traveling over or stored on University information systems has occurred. We do not purport to offer an exhaustive account of all past access. We instead intend to describe the basis for our conclusion that access has historically occurred only in limited circumstances.

1. Existing Limits on Mechanisms for Accessing Information: On the one hand, access can be automated, in which case only a program directly accesses user information. Alternatively, access can be carried out directly by people so that they are able to view original user data with their own eyes. The information accessed can be similarly categorized. Information can take the form of low-levels of abstraction or representation (e.g., bits and bytes) or at higher levels of abstraction in forms that are more meaningful to humans (e.g., human language and images).

Special concerns arise if humans directly view user information in its human-understandable form, such as when a person actually reads an email message or its header content. Other forms of access, such as algorithms that process Internet addresses, Web browsing histories, or email destinations and contents may also raise concerns depending on the use made of the results of those algorithms. Moreover, when a program processes information, it may produce higher-level information (e.g., aggregate statistics on network bandwidth) or filter out information (e.g., IP addresses) so that human operators are insulated from personal information. Generally, there is less concern when programs process data, as long as the information the programs extract does not reveal personal information. Of course, whether a machine or human accesses information, it is vital that the access occurs for an appropriate

purpose and with proper authorization, and that any information collected is adequately secured.

In order to respect sensitivities, Harvard's current information technology practices strictly limit the circumstances in which system administrators observe user information in human-understandable form. Instead, Harvard's current practices permit humans and machines routine access to information only in the least readable form required to perform maintenance, backup, and monitoring of the network for information security threats (e.g., aggregate traffic flows, not content or text). In addition, only information technology staff assigned to particular systems get access to information on those systems, and information technology staff members are trained to avoid access to user information whenever possible. For example, three trained engineers monitor the network for patterns of attack and malware and rely most often on aggregated machine-generated information in performing such monitoring. Unlike some commercial services whose business relies upon advertising or selling information about users to third parties, Harvard and its information technology staff do not have a practice of retrieving email content or other electronic information in order to track individual user behavior.

2. Limited Purposes for Which Access Has Been Authorized in the Past: An understanding of how infrequently access occurs also helps to put the University's technical capabilities in proper perspective. Although records of prior occasions for obtaining access are spotty, and the system for tracking them is decentralized and underdeveloped, we have done our best to reconstruct past practice, with the assistance of the Office of the General Counsel and Harvard University Information Technology Services. The best information available to the Task Force suggests that, over the past five years, across all Schools and components of the University, instances of access occurring without prior consent are rare, especially with respect to the most sensitive forms of access. The record also shows that there has at no time been a systematic University policy of monitoring email or Internet usage, or scanning files kept on University devices or servers for reasons other than system maintenance and protection.

More specifically, the record shows that access to information occurs primarily for system maintenance and protection (such as by scanning with anti-virus software). The other occasions are best described by category.

a. Business Continuity: It appears that, other than system maintenance and protection, the majority of instances of access over the last five years concerned efforts to ensure business continuity. An example would be a circumstance in which information concerning University financial matters is on the computer account of an employee who is unavailable. It appears that most of these occasions occurred with the awareness of the user, in part because the practice is widely known among staff, who are the overwhelming focus for obtaining access for the purpose of maintaining business continuity.

b. Academic Misconduct: The next largest category involved research misconduct and grant compliance investigations. It appears that access to electronic information for this reason

occurred less than 15 times over this five-year period and in each instance in accordance with the established committee process for handling such inquiries and investigations. In many of these cases, and perhaps all, access occurred with notice to the affected parties. In a number of research misconduct or grant compliance cases, the only action involved the sequestration of the information (in other words, the isolation and freezing of that data so as to make it available for a search) rather than access, and here, too, notice occurred in many if not all instances. There have also been occasions when access was sought in connection with academic misconduct investigations involving students pursuant to Administrative Board actions. These appear to have been carried out with consent. There have also apparently been cases of accessing log information to determine whether student papers were turned in to faculty when claimed, apparently with advance consent and notice, though there may be instances of which we are not aware in which that may not have occurred.

c. Legal Processes: The final significant category of cases involves compliance, under the supervision of the Office of the General Counsel, with subpoenas from law enforcement or attorneys involved in civil litigation or in cases where the University itself must prepare for litigation or comply with discovery obligations. Relatedly, there are rare cases where information has been provided in response to law enforcement requests in connection with ongoing investigations.

d. Other Purposes: The Task Force is aware of few instances that—like the access authorized last spring to identify a potential disclosure of confidential information—fall outside any of these categories. Most of the fewer than 10 instances over the last five years occurred in the course of staff misconduct investigations. Such cases might concern, for example, missing property.

Conclusion

As the foregoing review indicates, Harvard possesses the capacity to access electronic information that travels over, or is stored on, its information systems. That does not make Harvard unusual. In numerous settings, people communicate and store information through electronic means that expose that information—albeit often only in the form of bits and bytes—to those who own or administer the information systems and devices. In light of this reality, "privacy" does not exist in precisely the same way it once did. In the past, writing, conversing, and communicating did not inevitably and routinely entail that the contents of those communications or even related data might be available to anyone beyond intended recipients. Now it does. Thus, today, those who use University systems and devices often communicate in writing in a way that is extremely convenient but that unavoidably gives the University the potential capacity to access that information.

This shift in practice does not mean access should always be permissible. In determining the appropriate rules for permitting access to this information, we must look beyond the fact that

the University owns, provides, and/or administers the information systems and devices. Rather, the increased capacity for access heightens the need for policies and protocols that structure and constrain decisions about when and how such access may occur.

II. Guiding Principles

In considering the rules governing access, the Task Force did not view its objective as an operational or managerial one. To be sure, a policy must be designed so it does not impede the University's ability to conduct its operations in a practical manner that serves both its mission and the members of the University community. But a policy must also reflect the fact that sensitive decisions regarding access, if made without proper forethought or conformity with appropriate limitations, can create significant and justifiable concern within the University community.

The Task Force identified three animating principles to guide its recommendations. It is important to state these principles at the outset as they support the analysis and recommendations that follow.

Candor

The first principle is candor. The Task Force believes that it is critical that University policies are transparent about the University's legitimate needs and its technological capabilities. Users of University systems, networks, and devices should be aware of the technical capabilities of system administrators. Users should also be aware that in some circumstances the University may need to access electronic information in order to fulfill the University's responsibilities. Members of the community should also know about the protocols and processes that regulate when access may be allowed, and how information may be accessed. A policy that provides such transparency—even if at points it merely makes clear that the lines regarding access are necessarily somewhat fuzzy—enables members of the community to make informed judgments in using the University's information systems, networks, and devices.

Trust

The second principle is trust. It is not sufficient for a policy to provide clear notice of when and how access to electronic information may occur. In substance, the policy must also be consistent with, and true to, the mission of a research university like Harvard. That means the policy must provide safeguards against unwarranted access that reinforce trust within the community. Users of the systems, networks, and devices must feel confident that they can use these means of communicating in the course of engaging in the range of activities and pursuits that a university, uniquely, seeks to foster. A university community cannot retain its vibrancy absent that sense of trust among its members.

Respect for Academic Freedom

The third principle is respect for academic freedom. Specifically, a policy in this area should be designed to facilitate not trust in the abstract, but the kind of trust that enables the pursuit of learning and the production of knowledge. Any such policy must therefore be conducive to an environment that supports intellectual ferment, the sharing of ideas, risk-taking, free thought, and academic freedom. A policy limiting access should thus ensure that the technical capacity to access sensitive user information does not result in decisions to access that information for purposes antithetical to the University's core academic values and best academic traditions.

Conclusion

These principles—candor, trust, respect for academic freedom—are in many respects reinforcing. But there are potential tensions among and between them. Accordingly, a full appreciation of these principles requires certain trade-offs in application. The discussion that follows discusses these trade-offs, in light of these principles, in the course of analyzing the issues that would likely need to be resolved in making a decision about whether to authorize access in any particular case.

III. Purposes Supporting Access to Electronic Information

The threshold question in any particular case is whether there is a substantive justification for permitting access. The Task Force believes that such a justification must be rooted in the purpose that would be served by accessing the information at issue. Thus, the Task Force rejects the view that either the technological capacity to effectuate access, or the status of the user whose information might be accessed, should determine whether a request for access is justified.

Capacity for Access Cannot Justify Access

An appropriate respect for system users suggests the virtue of the following rule: No access should be permitted merely because technology makes it possible to obtain such access. This point is worth stating explicitly even though it may seem obvious. Expectations are not simply a function of what technology permits. Access will be seen as legitimate within the University only if a sufficient reason exists for allowing it. Correlatively, though, our discussions with a wide range of actors within the University convince us that access will be widely regarded as legitimate when supported by a sufficiently strong reason that is consonant with the University's mission.

A User's Role in the University Does Not Determine the Legitimacy of Access

The Task Force does not think it advisable to root a policy regarding access in the status of the user, such that, for example, access would always be permitted for staff but not faculty.

Of course, the legitimacy of a decision to grant access may—and often will—be related to the formal status of the user. Academic freedom concerns are more salient for some users within the community than for others. Those performing staff roles will expect access for operational reasons to an extent that students and faculty ordinarily will not. Still, the justification for, and contours of, any particular decision to obtain access should not be wholly determined by a user's status. The touchstone should be the soundness of the reason the University seeks access, regardless of the status of the user.

As a practical matter, an emphasis on the reason or purpose for the requested access helps keep the inquiry focused on the proper question and thus away from distracting judgment calls. As illustrated by the recent controversy over access to emails of resident deans, statuses blur and are not always easy to classify. In addition, members of the University community play multiple roles. Students may assume staff roles, faculty may perform administrative tasks, and administrators may teach courses or undertake academic projects. Communications between persons also often cross roles—students communicate with faculty, faculty with staff, and so on. A distinct policy for each role or status would inevitably generate confusion and focus attention on the propriety of the classification rather than the reason for seeking access. At all times, the key question—in light of the need to promote candor, foster trust, and respect the academic mission of the University—should be whether there is a good and sufficient reason to grant access.

Need to Show That the Purpose Would Be Served by Granting Access

One additional point bears emphasis. The identification of a legitimate purpose does not, standing alone, suffice to justify granting access in a given situation. University personnel must also consider whether there is a sufficiently substantial factual basis to support the judgment that granting access would actually further the purpose that the request for access is meant to serve. University personnel should also determine whether reasonable alternatives to obtaining access would serve the University's legitimate institutional needs. For example, an investigation may be resolved satisfactorily through further inquiry and discussion with a person, thus obviating any need to seek access to electronic information. In addition, nonconsensual access can be avoided in many instances by obtaining consent in advance.

Nonetheless, there are circumstances in which there is a sound factual basis for the asserted need for access and neither reasonable alternatives nor consent are available. In those circumstances, the critical determination is whether the purpose that grounds the request for access is legitimate.

Difficulties in Formulating an Exhaustive List of Legitimate Purposes

Any effort to name in an exhaustive manner the purposes that might support and legitimate a decision to grant access to electronic information confronts a difficulty. Even though it is obvious that not just any purpose will suffice to justify access, in the rapidly evolving

worlds of higher education and electronic communication, there are too many unforeseen circumstances to permit a closed list. And yet, there is a risk that an open-ended list will provide no guidance as to the kinds of purposes that are, in the eyes of the University community as a whole, sufficient to justify obtaining access.

For this reason, proper application of this aspect of the policy, as is true of other of its aspects, will require a sound institutional structure. Proper application will also depend upon the exercise of sound judgment of actors making decisions within that institutional structure. We set forth recommendations concerning that structure in subsequent sections of this report. But precisely because a policy that relies exclusively on open-ended language to specify the limits it purports to identify runs the risk of failing to provide adequate guidance, we do seek to describe with greater particularity the kinds of purposes that we believe count as legitimate.

We do so by setting forth an *illustrative list, drawn from past University experience, of particular purposes that justify access*. This list, because it is illustrative rather than exhaustive, allows for the possibility of justified searches for purposes other than those that it explicitly describes. However, the policy should make clear that any such additional purpose must be of comparable appropriateness to those listed below. Identifying such a list helps to make clear the range of circumstances in which there seems to be a broad consensus about the legitimacy of obtaining such access. The express identification of those circumstances can thus help to anchor and test more difficult judgment calls about the legitimacy of other possible purposes that may be asserted.

This approach is by no means a perfect solution to the drafting difficulty, but there is no perfect solution. We think it preferable to provide this level of specification rather than to simply lump the various possible legitimate purposes together by providing that the University may search for any reason it deems "appropriate," for any reason that serves a "legitimate University purpose," or, similarly, to avoid any "harm" to the University. Formulations like these can be found in current University policies. They are also found in the privacy policies of peer institutions of higher education and at other large organizations. Such broad formulations, without more specification, obscure more than they illuminate. They offer little insight into what counts as a "legitimate" purpose or what constitutes the kind of "harm" to the University that would justify authorizing access to the data at issue. It is important, therefore, to explain, to the maximum extent possible, those distinct purposes for permitting access that the University believes *are* legitimate, even if it is not possible to fully specify all of those purposes and even if those purposes are themselves subject to some interpretation regarding their scope.

Examples of Legitimate Purposes for Granting Access

There are clearly instances in which accessing electronic information would not be appropriate. It would obviously be inappropriate for administrators to gain access as part of an effort to dissuade a faculty member from writing a scholarly article critical of the University,

even though the University owns the system or device on which such information may reside. Similarly, there is no justification for a practice of continuous, indiscriminate monitoring of systems and devices for data (other than scanning for system protection and maintenance) that might possibly be "harmful" to the University, and the University has never had such a policy in place nor considered adopting one.[4] In this respect, the University is clearly different from other types of employers, where such continuous monitoring does occur. At the same time, there are purposes that are clearly consonant with the University's mission and sufficiently important to warrant access. We list them below.

1. Protecting the life, safety, and health of a member of the University community. The paradigmatic case for obtaining access is that of a missing student who is feared to be in danger or that of an emergency situation in which members of the University community are in danger while on campus. Access to electronic information tailored to this purpose is appropriate in that it may provide crucial information in locating the student or resolving concerns about his or her apparent absence or in identifying the nature and source of the threat to the campus. It is difficult to identify all the cases of a similarly extraordinary nature that implicate the life, safety, and health of a member or members of the University community. Similar cases, however, also provide a legitimate basis for obtaining such tailored access.

2. Handling litigation or complying with legal process, such as subpoenas. The main requests for access of this type concern law enforcement investigations and discovery being conducted in connection with civil litigation, whether that litigation is brought against the University itself, by the University, or by or against third parties. There may also be similar types of requests from government agencies. The University, like any institution in our society, has an obligation to comply with legitimate demands for its assistance in law enforcement and other governmental investigations, and to permit the efficient functioning of the legal system, when those demands are made pursuant to established legal processes. (It is important to emphasize here that the University's obligations extend only to *legitimate* demands. As a result, the University is under a separate obligation to evaluate the legitimacy of particular demands and to resist those that it deems illegitimate, as has been the practice of the Office of the General Counsel.) Compliance with such requests, therefore, is a legitimate ground for accessing electronic information.

3. Protecting University information systems and devices from disruption and damage. The University's information systems, like those of any large institution, face major security challenges. Attacks on the system are steadily growing in volume and sophistication. The University must take measures to protect the system from such

[4] The only exception relates to University Health Services, which at times engages in certain monitoring practices that have their origins in the organization's distinctive responsibilities to protect patient privacy.

attacks, and those measures may entail scanning through electronic means the information that travels over University systems and through its devices. In addition, Information Technology staff may examine electronic data in a more focused manner in the event systems become infected with viruses or otherwise are corrupted. Here, too, the need to protect and maintain the University's systems constitutes a legitimate purpose for certain forms of access, such as certain types of automatic scanning.

4. Facilitating continuity of University operations. Another legitimate reason for access is the need for continuity in University operations. For example, an employee responsible for handling sensitive financial information for the University, or a component of it, might leave for employment elsewhere, or become incapacitated. Critical information may reside in the employee's computer files. While access perhaps may be obtained with the consent of the user if still an employee, there may be times when it is not feasible to obtain consent. Access for this purposes focuses on accounts of users performing administrative tasks. But it is also important to recognize that such administrative tasks may be performed, depending on the circumstance, by a variety of actors within the community—from students to tenured faculty. Thus, the business continuity justification for a search cannot be categorically limited to only one slice of the University community.

5. Facilitating internal investigations concerning misconduct. The University has an obligation to investigate certain credible allegations of misconduct, including academic and research misconduct. The need to conduct such investigations can justify the University in accessing electronic information in service of that investigation.

The broad range of activities that occur under the University's auspices, and the unusual responsibilities the University has to those whom it teaches and employs, makes it difficult to identify in advance the full range of circumstances in which an internal investigation may warrant a decision to authorize access. Such decisions will necessarily be dependent upon the facts and context.

This, too, creates a drafting difficulty. Granting access to facilitate internal investigations inevitably raises the greatest concerns because this purpose is potentially self-justifying: any effort to obtain access connected to any investigation could, in theory, be justified on the ground that it was related to an internal investigation. For that reason, permitting access for the purpose of facilitating internal investigations necessarily places significant reliance on other provisions of an electronic information policy, such as those that identify additional limits on, and establish procedures for, obtaining access for investigatory purposes.

These additional limits and procedures include the requirement that there be a sufficient factual basis for an investigation before permitting access to electronic information.

They also include the rules about who may authorize access, the provision of notice, and the implementation of after-the-fact review by a committee outside the direct chain of authorizing decision makers, which the report addresses in the ensuing sections. But we do think that identifying the limited purposes that have historically grounded the vast majority of decisions to grant access offers important guidance for assessing whether, in a particular case, an investigation is sufficiently important to justify authorizing access to electronic information.

Conclusion

A University policy should make clear that access should only be granted for a reason that is both important and legitimate in light of the University's mission. The mere fact that the University owns or administers the information systems should not lead University officials to conclude access is appropriate. Nor should decisions about access be made solely with reference to the role a user performs at the University. Instead, the policy should guide decision makers to think hard about whether the request for access, if granted, would serve a legitimate University purpose that is comparable in weight to those purposes that have historically supplied the basis for the vast majority of University decisions to grant access.

IV. Authorization: Who Should Make the Determination That Access Is Appropriate?

Wholly apart from the substantive criteria that should be used in assessing whether a request for access would be legitimate, a policy must also provide guidance as to who is empowered to apply those criteria and thus authorize access in a particular case. The issue of authorization, therefore, concerns who within the University possess authority to approve access to the electronic information of users, be they faculty, staff, or students.

Separating Authorizers from Implementers

The people entitled to authorize access should not be the people who do the technical work of implementing requests for access. The responsibility for carrying out access requests rests with senior Harvard University Information Technology personnel and School Chief Information Officers. Prior to obtaining access, therefore, information technology personnel should be required to ensure that the request for access comes from an authorized person *outside* of the information technology units. Such a requirement puts in place an additional safeguard to help ensure that access does not occur unnecessarily. It also helps ensure that those making decisions to authorize access are best positioned to consider the full range of issues that should factor into any such decisions.

Designating Who Can Authorize Access

The Task Force recommends the policy designate a limited and appropriate class of persons who are entitled to authorize access. Ensuring that only suitably high-level actors—such as the dean of a faculty or the head of an administrative component—are able to authorize access limits the possibility that access will be sought needlessly. It also promotes accountability. Authorization provisions are therefore a necessary complement to provisions addressing matters such as the reasons that justify access, the tailoring of access in light of the reasons for it, and the giving of notice to the person whose information is accessed.

That said, there are various types of access, and the role that authorization plays will vary accordingly. In some instances, the person whose information is being accessed will have consented to the relevant type of access and authorized the access. In addition, the Task Force envisions that the University will provide periodic general notifications of routine, automatic monitoring to detect viruses and other system threats. No additional authorization for this type of access should be required.

In some areas, moreover, there are already well-accepted procedures in place with respect to authorization, and we do not believe they should be revised. Investigations into allegations of academic misconduct are an example. For research misconduct and grant compliance investigations, individual Schools have established procedures for generating requests for access to electronic information, such as through faculty committees. In cases that involve compliance with legitimate requests as a result of litigation, there are also well-established procedures that have been developed by the Office of the General Counsel. The Task Force believes that those procedures are working well and recommends that they continue, subject to periodic review.

As discussed earlier in this report, business continuity accounts for the majority of instances in which information is accessed: for example, when financial information critical to the operation of some part of the University is stored on the computer of an employee who is unavailable. In such instances, the Task Force recommends that the relevant unit's chief human resources officer be responsible for authorizing access in the event consent has not been previously obtained. Given the special considerations of academic freedom that attach to faculty activities, in the circumstances in which faculty are performing staff or administrative functions, the Task Force's expectation is that the dean of the relevant faculty would need to authorize access to a faculty member's information even if the reason for access is business continuity.

Authorizing access to electronic information is a serious matter. For the infrequent instances where cases do not fall into the foregoing categories, therefore, the Task Force recommends that the power to authorize access be limited to the dean or, if not a School, to the head of the relevant unit, or an appropriate designee if the dean or head is unavailable. This is most obviously the case for instances of investigative access that occur without the consent of the user. This approach ensures the responsibility to authorize access rests with a member of the

relevant unit who has appropriately high-level responsibilities within its administrative structure. It also ensures a separation between those who authorize access and those who implement access requests.

It is not practicable, however, given the different types of access and different administrative structures within the University's units, to identify precisely the relevant decision-maker(s) for each unit. In addition, the designated approval process may be too cumbersome in certain exigent situations. To take an example drawn from recent experience, the Harvard University Police Department (HUPD) may seek access to electronic information in response to a credible exigent threat to campus safety. Insofar as access is sought where time is of the essence to prevent threatened harm, as opposed to investigating an incident after the fact, HUPD should attempt to obtain approval for such access from the Vice President and General Counsel, to whom it reports. In the very rare instance where it may not be feasible to obtain timely review of the request that way or from another senior University official (such as the Executive Vice President), the University's overarching interest in campus safety may be sufficient to justify providing HUPD with appropriate access to records. At the same time, it is important to keep in mind that, under the policy recommended by the Task Force, any decisions to authorize access will be recorded and will be subject to periodic review by an oversight committee that we further describe in a subsequent section of this report.

Consultation with Oversight Committee

As a practical matter, decisions regarding access will often be made in consultation with others, including the Office of the General Counsel. The Task Force did consider the possibility of mandating consultation with (or even approval by) the proposed oversight committee prior to the authorization of any request for access, or even for only those requests that pertain to internal investigations. That approach would have the advantage of placing more "eyes" on any decision to authorize access. The Task Force concluded, however, that the advantages of such a mandate were outweighed by the practical difficulties of implementation. The reality is that the most difficult judgment calls will often arise in circumstances where there are time sensitivities, and this point arose in many of our consultations. The Task Force is concerned that a mandate to consult with an outside committee would be too cumbersome, though that committee would be available for consultation if such consultation would be both practicable and useful. The Task Force is also of the view that the knowledge of after-the-fact review by an oversight committee provides a sufficient measure of accountability to ensure that judgments made in the moment are undertaken with appropriate prudence and caution.

V. Notice

Once a decision to authorize access occurs, the question of notice necessarily arises. An important aspect of our proposed policy, therefore, concerns the rules regarding when notice

must be given to the account holder or user. The Task Force believes there should be a strong presumption in favor of providing appropriately specific and timely notice.

The reason for adopting this presumption is straightforward. Notice provides a constructive form of transparency. It can help ensure the underlying reasons for access are appropriate. That is because the need to inform often carries with it the obligation to justify, which in turn lends discipline to the approval process. Notice is also consistent with the values of the University. It demonstrates respect for the members of the community and meets their reasonable expectations that they will be informed if their account is accessed. And it may help to narrow, or even eliminate, the need for access.

Consistent with these reasons for requiring notice, notice will often entail more than a general disclaimer that access to electronic information may be sought. Rather, notice should be specific to the individual situations where access is sought. Because the content and scope of notice will often be heavily context dependent, however, we hesitate to be too prescriptive. A policy regarding notice must also take account of the practical circumstances that attend different types of access.

System Maintenance and Protection

For certain purposes, the Task Force believes that notice through a general policy statement regarding University access will suffice. The leading example concerns access that occurs in the course of the work of HUIT and its counterparts in maintaining the University's systems and protecting against security threats to those systems. That work inevitably requires some access to account information, mainly in the form of automated scans for viruses and other potential threats. It is not practical for HUIT to give specific notice each time these activities touch a user's account—the automated scans are continuously occurring. In addition, the sensitivities implicated by such system maintenance work are ordinarily much diminished. It thus suffices for users to be made aware in advance of the general practice. We do not believe such general notice would suffice, however, in the rare circumstance where the reasons animating access for the purpose of information systems maintenance and protection become focused on the conduct of individual users.

Business Continuity

Similarly, the provision of general notice would suffice when access is sought for the purpose of ensuring business continuity. The routine functioning of University operations makes it impractical to impose other than general notice obligations in this context. Indeed, the very reason for obtaining access to ensure continuity of business operations is that an account holder has become unavailable, often in circumstances that would make the provision of specific notice very burdensome if not impossible. We understand that the University has operated in accord with this practice in the past without generating concern or controversy among employees. It would be advisable, however, to ensure that protocols are in place for ensuring employees, both

current and future ones, are aware of the University's need to reserve the ability to seek access for this purpose. As mentioned earlier, the Task Force is persuaded that staff members typically understand that electronic information may be accessed for reasons of business continuity. Other members of the community may not share this general understanding even though they, too, may perform some staff functions. In those cases, and in keeping with the principles outlined earlier in this report, the Task Force suggests it may be advisable to provide specific and timely notice to those users if access for the purpose of business continuity occurs.

Legal Bars to Notice

There are also cases in which the University may not be able to provide notice due to legal constraints. For example, notice restrictions often accompany subpoenas or other forms of legal process that the University receives. In such cases, if the restriction is legitimate, the University may not be in a position to provide specific notice.

Strong Presumption Favoring Notice

Outside these contexts, and especially concerning internal investigations, the University should have a very strong presumption in favor of providing specific notice to current members of the community when seeking access to electronic information. Any departure from this presumption should be in response to a compelling reason, and expressly authorized by the head of the School or unit who authorizes the access. The Task Force is of the view that, given the purposes served by notice, exceptions, if warranted at all, would be very rare.

The timing of notice also must be considered. In general, there are plainly reasons to strongly encourage providing advance notice. Doing so may obviate the need for access because the user may be able to provide the information through other means. It may also help serve the goals of minimization. The user may be able to identify the general or specific location of the information in question, making it possible to conduct a more targeted search. In addition, it will often be possible to provide such advance notice without compromising an investigation. Information technology systems permit system administrators to take a "snapshot" of a user's account, and thus the University often will have the ability to preserve the user's account and give advance notice to the user before specific access occurs. This has been the longstanding and uncontroversial practice in research misconduct cases, where records are impounded either simultaneously with or immediately before the faculty member is informed of the investigation.

Still, the Task Force is aware that occasions could arise in which the University may legitimately decide that advance notice is not appropriate or feasible. The very reason that grounds the authorization for obtaining access in some cases may make it impractical to give effective notice within the time constraints that warrant access in the first instance. That could be because the need for access arises from the unavailability of the person whose information needs to be accessed. Or it could be because giving notice may prematurely disclose the fact of the investigation and thus compromise its effectiveness. Based on the information provided to us

about historical practices, we expect these situations to arise rarely. If they do, however, University officials act appropriately in delaying notice, though any delay in providing notice should be authorized by the head of the School or unit (except in business continuity cases where a different authorization process is more appropriate) and the user should be informed as soon thereafter as reasonably possible—e.g., when the risk to the integrity of the investigation has passed.

VI. Ensuring That Access Occurs Only Through Narrow Means

When responding to an authorized request, information technology staff should ensure access occurs only in a narrow manner that avoids unnecessary intrusions and disclosures. Access should thus be minimized both in terms of the amount and type of information examined and provided, and in terms of the number of individuals who are allowed access to the information. In order to ensure both aspects of minimization, the Task Force recommends developing a clear and enforceable minimization protocol and a code of conduct for information technology staff, though in any particular case the person designated with the responsibility for authorizing access should also be involved in the effort to ensure that access occurs in an appropriately narrow manner.

The Task Force is impressed by the seriousness with which the University's information technology staff carry out their obligation to respect the sensitivities involved in this area. The following recommended protocols build upon and codify existing practices at the University. They also reflect recognition of the University's special academic mission, and thus they are aimed at ensuring such respect remains rooted in the University's information technology culture and practices.

Protocol to Minimize Access

The University Chief Information Officer (CIO) and School and unit CIOs should be held responsible for reaffirming that there are no other reasonable alternatives to obtaining access to requested data and ensuring that access to electronic information occurs only through narrow means. Although the nature of requests, the types of data requested, and the technologies that store data vary widely, a common protocol can be defined and applied consistently. We note that the following recommended protocol should be followed and further refined as the nature of requests, information, and technologies change.

- **Select specific variables that will meet the objectives of the request.** To ensure that information will not be unnecessarily uncovered or exposed, access should, absent extraordinary circumstances, be limited to specific information items (e.g., a single file or email message) as opposed to a broad technology category (e.g., hard drive or account). The specific date or a narrow range of dates that would be associated with the information and as many keywords as possible that characterize the information being sought should be used to minimize the results. Such specification should be reviewed by

at least one other person to determine whether there is a more constrained way to seek the targeted information. Whenever possible, the filtering of the data should be performed in an automated fashion as opposed to human "eyeballing" and comparison of results.

- **Limit execution to essential personnel.** The number of staff involved in the access must be limited as much as possible; moreover, only those staff who are trained in the techniques of information access minimization and who are fully aware of the consequences of abuse of such access should be authorized to participate.

- **Protect and secure any accessed data.** Any information that is produced by an authorized access must be protected and secured in a proof fashion, along with the mechanisms and descriptions used to produce the set of information accessed.

- **Record, track, and report all searches.** All authorized access should be reported promptly to the University CIO, who should be responsible for compiling University-wide results. The reports should be available to the oversight committee, mentioned earlier and described in the next section of this report, which can also help determine record-keeping protocols and whether and how summaries of this information can be shared further with the community.

IT Code of Conduct

All Harvard information technology staff should be expected to abide by a code of conduct that makes clear their responsibility to protect all electronic information they access while performing their duties. The code should further stipulate that information technology staff will obtain only the electronic information needed to do their job; they will use the information only for the purpose for which it was obtained; they will properly protect any information in their possession; and they will dispose of the information properly once it is no longer needed for business purposes. To ensure that the protection of users' electronic information is deeply rooted in the information technology services culture, all information technology staff should be trained in the code of conduct and how it specifically applies to their work. Additionally, an annual acknowledgment of the code and understanding that any violation of the code could lead to grounds for disciplinary action including dismissal should be implemented and sustained.

VII. Oversight and Auditing

We have argued that it is not practical to list all situations that may lead to a legitimate reason for the University to access electronic information through the University's information systems. Unanticipated situations will undoubtedly arise, especially with rapid changes in our

technology landscape. Furthermore, timely access can be crucial in certain situations, such as when there is an imminent safety threat to the community. When confronted with such a predicament, appropriately authorized individuals must rapidly determine whether and what access should be allowed. We believe that, based on our own examination, these situations arise rarely. But there is no careful record to confirm this belief, and that absence, coupled with a lack of a clear policy, has caused some mistrust. It is therefore important to develop processes that will give confidence that decisions in this area are made with the requisite seriousness.

To ensure that access decisions are not taken lightly, and that the heat of the moment does not cloud judgment, we recommend a combination of careful record-keeping and periodic post hoc review by a review committee that stands outside the chain of authorization. In particular, we recommend that a central agency, such as HUIT, should be responsible for, as a matter of routine, compiling a record of the kind of access that has been authorized, who authorized the search, the justification for the access, and any notice given. Establishing such records will require HUIT to work with other CIOs at the University, as well as with the oversight committee, to ensure that protocols and standards are in place to keep proper records in real time. Recording these facts will help ensure that appropriate steps in the access policy are being followed.

As noted, we recommend that the University form a small review committee whose job is to periodically review the access records. The committee should provide an annual report to the President regarding the cases. The members of the committee should include faculty. We believe that a review of this type will help ensure that authorizing agents will give careful consideration to decisions regarding access, even when under intense time pressure, as they will know that their decisions and approach will be subject to examination by an independent set of eyes. Where practical, an agent may wish to seek advice from the committee before granting access, though we do not recommend this as a requirement, due to the need for timely access in many cases.

Furthermore, we recommend that the review committee consider providing a distilled report to the broader community, indicating the number of different kinds of access that were authorized, either each year or every few years. This report must necessarily be presented in a manner that removes information regarding individuals. We are aware that there is some concern that the number of cases will be rare and distinct enough that an aggregation would still reveal information that should not be shared, especially if the report covered a single year as opposed to a longer time period. Until we have experience with careful record-keeping, we cannot know. Nevertheless, we think such a report should be carefully considered, in keeping with the policy's aim of promoting trust and candor.

VIII. Addressing Electronic Information Policy Challenges That May Arise in the Future

The University's access to the electronic information generated by faculty, staff, students, and alumni raises issues that are complex, sensitive, and hard to foresee. The Task Force's recommendations regarding access cannot fully address the whole range of concerns that pertain to access to electronic information. These issues include:

- adapting the policy to address new challenges that arise at the intersection of community values (candor, trust, and free and vigorous scholarly inquiry called respect for academic freedom earlier) on the one hand and evolving technologies and communication practices on the other, especially as the volume and type of electronic information grows, such as through the spread of online courses or the rise of so-called ephemeral forms of electronic communication, like Snapchat;
- ongoing review of the application and administration of the University's electronic communications policy, including the approval, oversight, and reporting of searches and access of electronic communications records;
- consulting and communicating with a range of members of the University community regarding the development and implementation of the electronic communications policy; and
- ensuring compliance with law, regulation, and partner policies regarding electronic records and communications.

In recognition of similar concerns, some large companies, as well as some universities, have established the role of the chief privacy officer, or CPO. The first CPO positions were created in corporations and have become fairly standard at technology firms. For example, Google, Microsoft, Mozilla, and Facebook have CPOs responsible for creating and implementing privacy policies that protect consumers. Among universities, CPOs are most often seen in institutions with hospitals—the University of Pennsylvania, Dartmouth, Columbia, and Brown all have a staff member with that title. Most typically, the duties focus on compliance with obligations in federal and state law to respect the confidentiality of certain information. The position often falls under the CIO or the compliance function.

Harvard does not presently have a chief privacy officer, and it may be that there is no need to create such a position at the University. Some of the issues raised in this report fall under duties conventionally executed by a chief privacy officer. However, many of Harvard's challenges—such as creating an electronic communications infrastructure that fosters community trust and advances academic freedom and research capability—are not necessarily within the traditional purview of chief privacy officers. Harvard's challenges in this domain extend beyond privacy to assuring the integrity of electronic communications.

Whether or not Harvard establishes a CPO, the Task Force is of the view that it is important to identify and implement a mechanism for performing in a sustained way the functions delineated above. That mechanism could involve new or existing administrators, presumably acting in conjunction with an advisory body that includes faculty members as well as other members of the University community (such as the oversight committee described above) to promote a sense of trust and accountability and ensure that a broad range of viewpoints and perspectives is considered. The aim is to avoid future controversies by anticipating the frontiers of policy in advance. Even with a CPO in place, the Task Force believes the oversight committee described above would perform an important independent advisory function.

IX. Conclusion

A chief concern of those with whom the Task Force met is that, at present, users and administrators find it hard to determine the University's policy in this area. Accordingly, the recommendations for a comprehensive University policy set forth in this report will only achieve their aim if any policy that results is known to, and understood by, both those responsible for administering it and those who use the University's electronic information networks, systems, and devices. The Task Force thus believes the policy's adoption must not mark the end of attention to the issues raised in this area. Attention must also be given to ensuring any policy is readily accessible, known, and appropriately internalized.

To that end, the Task Force recommends charging an identified actor within the University administration with ensuring that the policy is effectively implemented and disseminated to both existing and new members of the community so that they become familiar with it. Special efforts must also be made to ensure that those within the information technology community and those who may be potentially designated to authorize access fully understand the terms of the policy and its intended operation. The Task Force has not attempted to lay out the best means of achieving the necessary dissemination and communication because there are a range of options.

The Task Force does wish to emphasize the importance of ensuring that the University charges someone with the responsibility for overseeing the policy's operation, implementation, and dissemination. Only through an effective and ongoing process of educating the University community will the University achieve the underlying goal: ensuring that there is reason to trust that the University is handling decisions about access to electronic information in a manner that honors its best traditions and its special academic mission. At the same time, the Task Force believes that, with such a process for education in place, the adoption of the policy concerning access to electronic information that is set forth in this report would enable the University to realize that goal.

Appendix A

Electronic Communications Policy Task Force
Members

David Barron, *Chair*
The Honorable S. William Green Professor of Public Law
Harvard Law School

Patricia Byrne
Executive Dean
Harvard Divinity School

Emma Dench
Professor of the Classics and of History
Faculty of Arts and Sciences

Karen Emmons*
Associate Dean for Research and Professor of Social and Behavioral Sciences
Harvard School of Public Health

Ann Forsyth
Professor of Urban Planning
Harvard Graduate School of Design

Jeffry Frieden
Stanfield Professor of International Peace
Faculty of Arts and Sciences

Archon Fung
Ford Foundation Professor of Democracy and Citizenship
Ash Center for Democratic Governance and Innovation
John F. Kennedy School of Government

John Goldberg
Eli Goldston Professor of Law
Harvard Law School

Rakesh Khurana
Marvin Bower Professor of Leadership Development
Harvard Business School
Master of Cabot House
Harvard College

Jennifer Leaning
Director, François-Xavier Bagnoud Center for Health and Human Rights
Harvard University
FXB Professor of the Practice of Health and Human Rights
Harvard School of Public Health
Associate Professor of Medicine
Harvard Medical School

Appendix A

Nonie Lesaux
Professor of Education
Harvard Graduate School of Education

Barbara McNeil
Ridley Watts Professor of Health Care Policy
Harvard Medical School

Daniel Meltzer
Story Professor of Law
Harvard Law School

Richard Mills*
Executive Dean for Administration
Harvard Medical School

Greg Morrisett
Allen B. Cutting Professor of Computer Science
Harvard School of Engineering & Applied Sciences

Jonathan Lee Walton
Plummer Professor of Christian Morals
& Pusey Minister in the Memorial Church
Faculty of Arts and Sciences
Professor of Religion and Society
Harvard Divinity School

Staff to the committee

Marilyn Hausammann
Vice President for Human Resources
Harvard University

Robert Iuliano
Vice President & General Counsel
Harvard University

Anne Margulies
Vice President, University Chief Information Officer
Harvard University

Leah Rosovsky
Vice President for Strategy & Programs
Harvard University

**Left the University for other employment before the work of the task force was concluded.*

Appendix B

David Barron, *Chair*
The Honorable S. William Green Professor of Public Law
Harvard Law School

ELECTRONIC COMMUNICATIONS POLICY TASK FORCE

Charge to the Task Force

The task force will consider and recommend appropriate policies regarding access to, and confidentiality of, electronic communications that rely on university information systems. It will consult with faculty, staff, and students in order to obtain a full understanding of the perspectives of each group.

In undertaking its work, the task force will inform itself about policies now in place at Harvard and other relevant institutions and solicit perspectives and advice on best practices.

The task force will consider whether and to what extent Harvard's policies should be university-wide or specific to certain parts of the University or particular institutional roles and responsibilities.

The task force will be expected to focus on recommending policies for the future that are both principled and practicable and that account for the reasonable expectations of individuals, the legitimate interests of the University, and associated issues of notice and process. The task force is not expected to investigate or render judgments on past events, but rather to take general account of instructive examples at Harvard and elsewhere as one means to understand the complex of considerations that can inform sound recommendations for the future.