
PRIVACY POLICY

Academic Computing Center, Engineering Library (ACCEL)
College of Engineering, Cornell University

- March 15, 2006; revised May 14, 2006

Purpose:

1.0 This is an informal document that has been written to provide users of ACCEL with a description of what personal information is collected during normal operations, what policies we have to safeguard personal information users may store on ACCEL resources, and an outline of certain circumstances in which employees of ACCEL may either have access to or reason to proactively collect personal information about a user of ACCEL.

1.1 Please do not hesitate to contact any ACCEL consultants if you have any questions concerning this document: accel@accel.cornell.edu.

General Practices and Your Personal Information:

2.0 As a general principle, ACCEL employees attempt so far as it is reasonably possible to respect and protect the privacy of users of ACCEL.

2.1 This implies a general policy against proactive collecting of personally identifying information, insofar as it is reasonably possible. This means that ACCEL does not actively monitor user activity.

2.1.1 In certain limited circumstances, personally identifying information may be acquired. These circumstances include routine security analysis, analysis of aggregate bandwidth usage, and the enforcement of ACCEL anti-virus policies. (See 3.0 below)

2.1.2 However, for example, ACCEL does not proactively log what websites users visit, nor the programs they use.

2.2 ACCEL employees will only access a user's home directory when either,

2.2.1 such access is required by either superseding university policy and/or applicable law, or

2.2.2 when provided with written permission from a user to access their home directory.

2.3 In the event that ACCEL is required to access a user's home directory, unless otherwise obliged by superseding university policy or law, a reasonable effort will be made to inform the user of the occurrence of the access, an explanation of why the access was required, and what information was collected in the course of the accessing the user's home directory.

2.3.1 It is the *de facto* policy of ACCEL to attempt to provide such notice prior to the accessing a users home directory, but ACCEL offers no guarantee that it will always be able to do so.

2.4 Users are expected to respect the privacy of their fellow users. An attempt by one user of ACCEL facilities to access the personal information of another user will be treated *prima facie* as a violation of ACCEL policy, and may result in a suspension of privileges with ACCEL and further disciplinary action as provided for by Cornell University Policy.

Data We Collect:

3.0 ACCEL only proactively collects and stores information required for the operation of the computing facility.

3.1 This includes information a list of the users who are registered with ACCEL, whether they are currently logged onto ACCEL resources, the percentage currently used of the storage quota allocated to each user, an encrypted record of the user's password, and the user's account balance in ACCEL printing system.

3.2 This information is indexed according to the user's Cornell *net-id*. In certain cases, the user's legal name may be also associated with this information.

3.3 In normal circumstances, with the exception of automated scans for viruses and routine security auditing and analysis, ACCEL does not proactively monitor the usage of ACCEL computing resources by its users, nor the data they may choose to store in their home directories.

3.4 Certain extraordinary circumstances, such as the reasonable suspicion that ACCEL security has be breached, or that a user is engaging in the violation Cornell University Policy, as it applies to computing facilities, may result in ACCEL employees proactively collecting user data including, for example, IP traffic.

3.4 All users of ACCEL are provided with a home directory. ACCEL places no restrictions on what data may be stored their, and assumes no responsibility for the content of the home directory.

3.4.1 In certain cases, groups of users may be allocated *group home directories*. Though a group home directory may be made accessible to a number of ACCEL users, it is treated the same as a user's home directory for the purposes of privacy. (See 2.2 above)

3.4.2 ACCEL also routinely performs backups of all computing systems. These backups include both home directories and group directories, and

therefore in the course of performing backups, copies of a user's data may be made.

3.4.2.1 Backup copies of a user's home directory are treated no differently, for the purposes of protecting user privacy, than the home directory itself. (See 2.2 above)

3.5 Except when required to do so by Cornell University Policy and/or applicable law, ACCEL does not share the data it collects or stores with any parties outside of the administration of the College of Engineering.

Your Choices:

4.0 At any time, users may delete content from their home directory. However, an explicit request must be filed with ACCEL in order to have personal data removed from back-up records.

4.1 At any time, users may choose to terminate your account with ACCEL. This request will be processed as expeditiously as is reasonably possible.

4.1.1 Such a request may not lead to the expunging of a user's data from back-up records. (See 4.0)

4.2 At any time, you may ask an ACCEL employee about your rights and privileges as a user of ACCEL.

About This Document:

5.1 This document is subject to revision. ACCEL does not have a policy of notifying users of such revisions.

5.2 This document will be publicly available to all users of ACCEL.

5.3 Cornell University Policy has precedence over this document in the case of any conflict, either directly stated or as implied through a course of interpretation.