LIGO LABORATORY
MS 18-34
PASADENA CA 91125

TEL: 626.395.2129
FAX: 626.304.9834

MEMORANDUM

DATE: November 25, 2008

TO: LIGO Laboratory personnel
FROM: A. Lazzarini and J. Marx
SUBJECT: Right to privacy policy for LIGO Laboratory personnel
Refer to: M080370-v1

Summary

This policy provides authorized LIGO users with an expectation of privacy with regard to electronic communications, personal and confidential data. We provide restrictions on behavior for users and IT personnel who may have the capabilities to bypass controls and access protected data. This policy also provides for obligations on users to make efforts to control access to their private data, and on LIGO to enforce those mechanisms.

Introduction

The LIGO directorate believes that all LIGO staff and users should respect user privacy.

We recognize that our users may have electronic information stored on LIGO resources, and communications on LIGO networks, which they consider private or confidential. While we have an open science mission, researchers may at times consider prepublication results sensitive and may wish to maintain the confidentiality of that data until publication. LIGO staff may also maintain personnel and/or financial information. Additionally, we recognize that users may use LIGO systems for legitimate incidental personal use.

State and Federal law provide some obligations on LIGO to protect the privacy of certain information. LIGO also believes that we have an ethical obligation to respect our users privacy regardless. We do not wish to have environment in which people feel they are under surveillance.

LIGO provides users with the means to control access to their data and communications. However, certain LIGO staff have the technical capability to monitor user communications and bypass access controls on stored data. The LIGO directorate assures our users that those staff will user their capabilities only where and when expressly authorized. LIGO will consider violations of this policy as serious personnel issues which could result in disciplinary action. Therefore, this policy largely addresses the acceptable behavior of those with privileged access.

Purpose of Memo

This policy serves several purposes. It defines what data may be considered private and provides users with both a reasonable expectation of privacy and their obligation to take steps to assert the privacy of their data. The policy identifies restrictions on staff behavior where technical means cannot prevent access, and circumstances under which where those with privileged access may circumvent access controls.

Scope

This policy applies to all systems connected to LIGO Lab networks. Funding source or ownership for any particular system holds no relevancy to this policy. However, we grant some exception for particular critical or dedicated systems (detailed below) on which users should not maintain private data.

The policy also applies to all authorized users of LIGO networks with regard to their activity on these systems, regardless of the user's affiliation.

Expectation of Privacy

In order to provide users with an expectation of privacy, LIGO considers certain types of data implied personal or private, and prohibits accessing such data except as authorized below. Access does not imply authorization; users with the capability to circumvent access controls may not do so except for authorized activities.

Electronic Communications

LIGO considers all electronic communications private and confidential. We define "electronic communications" to mean data in transit over a network, and associated temporary storage during the transit process (e.g. RAM used for buffering). Federal law considers interception of electronic communications illegal except under particular circumstances, specifically "the protection of rights and property." Therefore, LIGO prohibits all users from monitoring of electronic communications except where authorized below. This prohibition does not include transactional information (e.g. mail delivery information, packet headers, etc.)

Stored Data

LIGO considers as personal information any data stored under a user's home directory which the user has not made readable to other users. We recognize that users may store work-related data under their home directories, but unless otherwise indicated or permitted by a user, others should treat all such data as personal. We also strongly encourage users to keep project related data outside of their home directories, to avoid having this policy interfere with the ability to support project and transfer ownership as necessary.

This policy should in no way imply that privileged users cannot delete private data as necessary for maintaining system resources, or when stored in an inappropriate location. Deletion of data without viewing the content does not result in a violation of privacy.

Email

LIGO also considers all email private and confidential. This status applies to email stored in folders, in transit over the network, and in temporary files during the delivery process.

Data openly published on personal web pages or otherwise openly accessible to all does not hold any expectation of privacy protection, as the user has explicitly relinquished his or her privacy protections by making the data public. However, we also recognize that users make mistakes and may unintentionally make personal or private data accessible to others. In those situations, when the data reasonably seems private or confidential, users should respect the privacy of the data and inform the user to make sure the exposure was intentional.

Confidential Data

LIGO considers Caltech personnel information and financial information as confidential regardless of who has access to it.

Credentials

We consider all credentials (including passwords), whether for users or systems, as private and confidential. We do not consider private or confidential the *identifiers* of those credentials (e.g. key fingerprints, public keys, x.509 Distinguished Names).

Exceptions

This policy also identifies a number of exceptions to the expectation of privacy.

Exempt accounts

This policy does not apply to data owned by "role," "system," or "service" accounts, rather, to data owned by an account specifically associated with a user or an account which processes user data (e.g. the "mail" account).

Exempt (Reduced Privacy) Systems

Some dedicated systems cannot provide access controls or individual accounts. In addition, LIGO maintains particular critical or special purpose systems on which we do not expect nor want personal activity or private data, even where users have individual accounts. On these systems, users should have little expectation of privacy. However, this lowered expectation does not absolve privileged users with respecting the privacy of any personal or confidential data which they might encounter, rather they should limit their activity to removing the data or asking the user to do so.

Education and outreach computing:

LIGO provides computing resources for K-12 education and public outreach, some in use by LLO Science Education Center staff, some available for visiting student groups, and others dedicated to particular permanent or temporary exhibits. We accept a special responsibility to ensure that LIGO Laboratory does not inadvertently expose children to harmful or inappropriate material. Our IT and outreach staff may therefore need to view and/or delete anything stored on these computers.

Computing resources dedicated to detector operation or automated data analysis:

LIGO dedicates computing resources to the operation or monitoring of critical hardware. For example, the CDS computers and networks at the observatories serve only to run the detectors and monitor relevant signals. In order to keep these critical systems clean and maintainable, we strongly discourage storage of personal files or information in dedicated systems. Because IT and scientific staff may examine any files or processes in this system in connection with their normal duties, users should not expect privacy in these systems, even when individual home directories are used. Nonetheless, as mentioned above, privileged users should respect personal items inadvertently left there.

Temporary use computing resources

LIGO provides computing resources for short-term or temporary use, such as public access computers in common areas, “loaner” laptops, and presentation systems. Users should not store private data on these systems nor have an expectation of privacy. LIGO staff may purge any user data on these systems on a regular basis.

Unauthorized users

Unauthorized users (i.e. intruders), unauthorized activities of authorized users, and anonymous users (those who legitimately access LIGO systems without authentication, such as web users) have no expectation of privacy.

Exigent Circumstances

Urgent situations may occur in which the time required to follow procedure for obtaining permission will result in a deleterious effect. Examples of such exigent circumstances includes those which could result in physical harm, damage to systems, loss or exposure of data, and interruption of service.

Legal Requirements

LIGO must comply with legitimate court orders. Fulfillment of those orders may supersede this policy.

Caltech Policy

We note that Caltech policy (http://hr.caltech.edu/policies/AUP.html) states that users have no expectation of privacy. In this regard, this LIGO policy goes beyond Caltech policy. However, Caltech management may at any time override this policy as needed.

Additionally, as this policy applies only to activity on LIGO networks, Caltech may monitor communications to and from LIGO systems which travel over other Caltech networks, consistent with Caltech policy.

Authorizations

As stated above, LIGO prohibits monitoring and access unless explicitly authorized under this policy. Capability to perform a particular activity in no way implies authorization to do so. We provide below authorizations for specific users to perform

specific activities. Users may not infer authorization for themselves based on the activity or authorizations of others.

Whom

System administrators must obtain explicit permission of the user, or the LIGO Directorate, before circumventing access controls (using privileged access) to access that user's files or email, or to change access permissions for the data. Third parties (e.g. another user, supervisors, etc.) may not attest to authorization of the user, nor provide a justifiable reason, even with the best of intentions.

System administrators may monitor network activity for the purposes of testing functionality and diagnosing system and application problems. Administrators should limit the monitoring to transactional information (e.g. IP headers) and not content unless absolutely necessary.

In circumstances where an administrator views private or confidential information, the administrator should respect the privacy of the user and not divulge that information to others.

The Chief Security Officer and his designees (the Security Team) may circumvent access controls and monitor network traffic as necessary to perform security activities as authorized in authorization memorandum LIGO-M070072. The CSO may authorize system administrators to assist in performing security activities.

LIGO Directorate, Observatory Heads, or the LIGO MIT Laboratory Director may request performance of monitoring and access for administrative investigation following Caltech policy and procedures, compliance with legal orders, or for performing payroll and other required personnel activities.

Obligations/Responsibilities

Effective Access Controls

In order to allow users to assert the privacy of their data, LIGO must make available effective access controls, control privileged access, audit trails to verify controls, and provide proper encryption tools and techniques. LIGO must also require access control settings for new user accounts make user data readable only to the user by default, so that the user must deliberately choose to make data public.

User Effort

Users must make an effort to protect their private, personal, or confidential data by making use of the provided access controls in order to assert protection under this policy. A user cannot choose to make data readable to "the world" and still have an expectation of privacy.

Project Data

In order to provide proper support for official projects, especially those which become production services, users should maintain the data for those projects outside of their home directories, with ownership and permissions appropriate for the project. Doing so

will avoid having this policy impede the transfer of support for projects when a user leaves or changes roles.

When questionable material or behavior is found:

When IT or other personnel come across material that could reasonably be associated with serious violations of Caltech, MIT or LIGO policy, or with possible criminal activity, they should immediately notify their line supervisor. The supervisor would then inform the Directorate and other appropriate offices, and then follow appropriate procedures to resolve the situation. If management carries out an investigation that involves IT resources, IT personnel may be called upon to assist; such personnel are not authorized to investigate on their own.

Departing Users

Users retain the privacy of their information after leaving LIGO Laboratory for any reason. However, LIGO will also expect those users to remove their private information before exit.

Media Sanitization

Anyone decommissioning media must destroy or sanitize the media before disposal. Anyone reusing media for another purpose must sanitize the media before reuse.

Education

LIGO will provide education and training on proper behavior for those who have privileged access. We encourage individuals to contact the CSO for guidance or assistance at any time.

Reporting

The LIGO CSO will report access or exposure of private data to affected users in a timely manner. This requirement includes access as authorized above, or unauthorized access when LIGO becomes aware of it. Some exception to this requirement may apply during compliance with court orders, personnel matters, and security and criminal investigations.

The LIGO CSO will issue an annual report to users on privacy practices, capabilities, and compliance with this policy.

Compliance with Institute Policy

As stated above, this policy provides LIGO users with privacy assurances above and beyond Caltech policy. Thus Caltech has the option at any time to supersede the LIGO policy. Additionally, once network traffic leaves LIGO networks, Caltech policy or the policy of the network provider to the sites will apply.

Applicable Laws

The following laws have guided the development of this policy.

18 USC § 2511, commonly known as “Title III Wiretap law”, makes illegal the interception of electronic communications, with an exception for service providers “incident to the rendition of his service or to the protection of the rights or property of the provider of

that service." Note that the exception applies to the provider, not the user of the service. The law also provides an exception for law enforcement with the appropriate court order. This law comes as part of the Electronic Communications Privacy Act

The Family Educational Rights and Privacy Act, commonly known as FERPA, obligates educational institutions to protect the privacy of student education records, including financial aid information, and provides rights to students regarding use of that data. LIGO's primary obligation from FERPA requires not publishing "directory information" about a student when student chooses to "opt-out."

California Civil Code 1798.29, 1798.82 and 1798.84, commonly known as SB1386, requires holders of "Personal Identifying Information" (PII) of California residents to notify the affected persons in the event of inappropriate disclosure of the information such as due to security breach. Caltech policy goes further to require notifying all persons affected, regardless of state of residency.

Definitions

Stored data

We define *stored data* as information written to storage media (sometimes called “data at rest”), such as hard disks, flash memory, etc. This definition includes RAM when used as a RAM disk. This definition does not apply to temporary storage for data in transit, such as RAM buffers, or mail queues.

Electronic Communications

We define *electronic communications* as data transmitted over a network (including a loopback network), or in the case of applications such as email, between two users. We differentiate between *transactional* information such as IP headers or mail transport agent logs, and the actual *content* of the communications (e.g. the IP packet “body”).

Private data

We use the term *private* data to refer to any data (defined below) considered personal, confidential, or sensitive.

Personal Data

We define *personal data* as any information not part of LIGO activities, such as email to friends or family, photos, etc.

Confidential data

We define *confidential data* as data belonging to LIGO or part of LIGO activities which LIGO cannot, or does not desire to, share with others. Examples include LIGO financial information and employee personnel and payroll records.

Sensitive Data

We define *sensitive data* as data non-confidential data, possibly available to a large number of LIGO affiliates, which LIGO does not want made generally available to the public, e.g. pre-publication measurement data.

Credentials

We define *credentials* as the information used to authenticate to a system. Credentials often have components considered *public* (e.g. public keys, usernames), and others considered *private* or *secret* (e.g. private keys and passwords). The protection of credentials stated above applies to the *private* portion of the credential.