

Responding to Compulsory Legal Requests for Information

Colleges and universities house servers, desktop computers, and data networks that store and transport a diverse array of data. With the stewardship of these services comes the responsibility to respond to compulsory legal requests¹ for information housed on and transmitted by these systems. Regular coverage by the press of data breaches, combined with shifts in the interpretation of the Communications Assistance for Law Enforcement Act (CALEA) of 1994, is contributing today to an environment in which institutional leaders are reconsidering institutional policies and procedures for handling such requests.

Legal Requests and Accompanying Issues

The members of the EDUCAUSE/Internet2 Computer and Network Security Task Force's Policies and Legal Issues Working Group has assembled "Protocol for Law Enforcement Requests: Guidelines for Responding to Compulsory Legal Requests for Information."² This resource provides concise explanations of compulsory legal requests, identifies common issues that may surround those requests, and offers a list of quality information sources for further information.

There are a number of types of compulsory legal requests: subpoenas, search warrants, court orders, and national security letters. Requests differ in the amount of time an institution is given to respond. Subpoenas may allow time to prepare materials, whereas warrants may require immediate responses. The issuing parties of compulsory legal requests vary based on the type of legal or administrative pro-



Illustration by Gemma Robinson, © 2007

ceedings involved. Additionally, public colleges and universities are also subject to public records or freedom of information statutes and thus may need to make records available on request.

Once requests come in, it is important that they be carefully reviewed for appropriate jurisdiction and that formalities be properly observed. Formalities include official signatures, designated delivery methods, credentialed delivery people, and service to an appropriate recipient. In contrast to other compulsory legal requests, public records requests may be much less formal in nature, and an anonymous oral response may be sufficient. Just as institutional representatives should be sensitive to the various types of information requests, the nature of the information requested should have some bearing on the disclosure process.

The data that are housed on servers and desktop computers or that traverse institutional networks are diverse in nature. In

some ways it is easiest to account for data stored on centralized, institutionally owned servers or for data that are associated with the business of an institution. In a number of cases, federal laws provide a degree of guidance for handling certain classes of information. The disclosure of student educational records is governed by the Family Educational Rights and Privacy Act (FERPA) of 1974. Protocols for the disclosure of electronic communications are established in the Electronic Communications Privacy Act (ECPA) of 1986. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 governs processes for the disclosure of medical records.

Careful consideration is also warranted for protected research data. For example, in the United States, some federal agencies have the latitude to issue certificates of confidentiality that are intended to protect the privacy of research study participants. Researchers may apply to the National Institutes of Health for

certificates of confidentiality when they collect sensitive biomedical, behavioral, or clinical data. In fact, the application process for a certificate of confidentiality requires that the principle investigator and an institutional representative sign a statement ensuring that the institution will use the certificate of confidentiality “to protect against the compelled disclosure of personally identifiable information and to support and defend the authority of the Certificate against legal challenges.”³ Once a certificate of confidentiality is awarded, decisions concerning the disclosure of protected data are in the hands of the primary investigator associated with a given research project. Certificates of confidentiality are just one example of protected research data and are illustrative of the importance of inventorying protected data on campus.

Policy and Decision-Making Issues

In spite of the complexity involved in receiving and assessing requests, institutional leaders should consider having a single point of contact for all compulsory legal requests.⁴ An appropriate single point of contact increases the likelihood that all requests for information will be handled consistently and appropriately. A single point of contact also necessitates the careful coordination of efforts, as well as preparatory work.

Cornell University has documented its approach to handling legal requests by having in-house counsel serve as the primary contact for compulsory legal requests.⁵ Other institutions without legal counsel on staff might consider a senior administrator who has ready access to out-of-house counsel and is well versed in institutional policy and decision-making structures.

Given the limitations of any single point of contact, it is important for an institution to articulate

- the nature and kinds of records and information that are maintained on campus and that are likely to be requested;
- the nature and structure of the institution's recordkeeping systems, including but not limited to its IT systems; and
- the institution's record retention policies and other institutional policies and state and federal laws that govern

the maintenance and disclosure of records and other information.⁶

The process of pulling this information together will require coordination among the offices and individuals who own the data, systems, and networks involved. A minimal list of relevant offices should include those with responsibilities for records on students, employees, campus security, research, purchasing, and accounts, as well as offices providing IT services within the institution. Institutions with research compliance committees may want to work with them in identifying projects that include protected research.

Conclusion

One important step in ensuring consistent institutional responses to requests for information is to establish a single point of contact to receive compulsory legal requests. Given the variety of these requests, as well as the diversity of protocols dictated by data type, coordinated efforts will be required to assess the nature and kinds of records on hand. Information is the lifeblood of the academy. Stewards of data and of the infrastructure through which they are transmitted thus need to think very carefully about how best to take efficient, responsible, and informed action in response to compulsory legal requests for information.

Notes

1. For the purposes of this article, “compulsory legal requests” refers to requests associated with law enforcement investigations, civil litigation, or public records requests.
2. Steven McDonald and Andrea Nixon, “Protocol for Law Enforcement Requests: Guidelines for Responding to Compulsory Legal Requests for Information,” December 2006, <<https://wiki.internet2.edu/confluence/display/secguide/Protocol+for+Law+Enforcement+Requests>>.
3. National Institutes of Health, Office of Extramural Research, “Detailed Application Instructions for Certificate of Confidentiality: Extramural Research Projects,” March 15, 2002, <http://grants.nih.gov/grants/policy/coc/appl_extramural.htm>.
4. McDonald and Nixon, “Protocol for Law Enforcement Requests.”
5. Cornell University, “IT Policy Flow Chart: Requests from Law Enforcement,” June 20, 2006, <http://www.cit.cornell.edu/oit/policy/calea/CALEA_Compliance.ppt>.
6. McDonald and Nixon, “Protocol for Law Enforcement Requests.”

Andrea Nixon is Special Project Manager/IT Strategist at Carleton College.



EDUCAUSE

Transforming Education Through Information Technologies

EDUCAUSE, a consolidation in 1998 of Educom and CAUSE, is a nonprofit consortium of colleges, universities, and other organizations, dedicated to the transformation of higher education through the application of information technologies. Through direct services and cooperative efforts, EDUCAUSE assists its members and provides leadership for addressing critical issues about the role of information technology in higher education.

EDUCAUSE Board of Directors

John E. Bucher, Chair

Director of Information Technology
Oberlin College

David L. Smallen, Vice Chair

Vice President, Information Technology
Hamilton College

Rebecca L. King, Secretary

Director for Information Systems & Services
Baylor University

Tracy M. Mitrano, Treasurer

Director of IT Policy and Computer Policy and Law Program
Cornell University

Jerry D. Campbell

President
Claremont School of Theology

John C. Hitt

President
University of Central Florida

Lucinda T. Lea

Vice President for Information Technology & CIO
Middle Tennessee State University

Marilyn A. McMillan

Associate Provost and Chief Information Technology Officer
New York University

Margaret F. Plympton

Vice President for Finance & Administration
Lehigh University

Kathleen C. Santora

Chief Executive Officer
National Association of College & University Attorneys (NACUA)

Scott E. Siddall

Assistant Provost for Instructional Resources & Director of Instructional Technology
Denison University

Ellen J. Waite-Franzen

Vice President for Information Technology
Dartmouth College

Ex Officio Member

Brian L. Hawkins

President
EDUCAUSE