Privacy Policy Framework

"Privacy is fundamental to the University. It plays an important role in upholding human dignity and in sustaining a strong and vibrant society. Respecting privacy is an essential part of what it means to be a good citizen, whether as an individual or as an institution."

The UW-Madison needs to create an integrated privacy policy framework, one that covers various aspects of privacy.

Resolution:

"Establish a UW-Madison Privacy Task Force to perform a comprehensive review of the University's current privacy policy framework and to make recommendations about how the University should address related near-term policy issues and longer-term governance issues. Specifically:

- An overarching privacy framework that enables UW-Madison to meet statutory and regulatory obligations in a manner respectful of individual privacy;
- Governance, implementation, and accountability structures across the University with respect to privacy and information security;
- A formal, ongoing process through which the University can examine and, where necessary, address through policy vehicles the technical and societal changes that have an impact on University policy and practice in the areas of privacy and information security; and
- Specific actions or phases needed to implement the proposed framework as University policy.

The Task Force will make recommendations to the ITC. It will include faculty – including ITC faculty – and campus officials with related knowledge and responsibilities."

The following are excerpts from the recommendations of the University of California (UC) Steering Committee on privacy policy framework. These recommendations can serve as a model for a UW-Madison privacy policy framework.

The only "edits" the UC Steering Committee recommendations include replacing "University of California" with "UW-Madison" and "California" with "Wisconsin." (Some of the quotes above are taken from the UC report.) The UC report is attached:

PDF

uc-privacy-and-information-security-steeri

I. INTRODUCTION

Background

Privacy is fundamental to the University. It plays an important role in upholding human dignity and in sustaining a strong and vibrant society. Respecting privacy is an essential part of what it means to be a good citizen, whether as an individual or as an institution.

Academic and intellectual freedoms are values of the academy that help further the mission of the University. These freedoms are most vibrant where individuals have autonomy: where their inquiry is free because it is given adequate space for experimentation and where their ability to speak and to participate in discourse within the academy is possible without intimidation. Privacy is a condition that makes living out these values possible.

Privacy is also a basis for an ethical and respectful workplace, one that is as aligned with the culture and expectations of the millennial generation and beyond, as it is with today's workforce. Such a workplace becomes a competitive advantage for the University.

Privacy, together with information security, underpins the University's ability to be a good steward of the information entrusted to it by its 43,000 students and 23,000 employees, and by its extended community of patients, alumni, donors, volunteers, and many others.

Protecting privacy, however, is challenging—for many reasons. It is a complex and subtle concept that makes definition elusive. The "consumerization" of technology drives expectations of "anytime, anywhere" access to bank accounts, medical test results, personal data files, course materials, and professors; and speaks to work/life balance. The ubiquity of cellphone cameras exemplifies and underscores a shift in the ability of individuals to affect one another's privacy. Social media paradigms create vast virtual communities that intersect with "real" life in unexpected ways, many of them privacy related. Information such as browsing histories, IP addresses, and location information are routinely captured and may be correlated, contributing to a more comprehensive and invasive view of an individual's activity. The management and curation of "big data" introduces a new class of "information" requiring privacy considerations. Investigators—and their funding agencies and publishers—may consider data collected in the course of their research to be confidential, at least for a limited period of time, whether or not they are about individuals.

Approach

The proposed privacy policy framework is guided by the following principles:

- We must maximally enable the mission of the University by supporting the values of academic and intellectual freedom.
- We must be good stewards of the information entrusted to the University.
- We must ensure that the University has access to information resources for legitimate business purposes.
- We must have a University community with clear expectations of privacy—both privileges and obligations of individuals and of the institution.
- We must make decisions within an institutional context.
- We must acknowledge the distributed nature of information stewardship at UW-Madison, where responsibility for privacy and information security resides at every level.

The proposed recommendations address three components:

1. An overarching privacy framework that enables UW-Madison to meet statutory and regulatory obligations in a manner respectful of individual privacy;	All recommendations
2. Governance, implementation, and accountability structures across the University with respect to privacy and information security;	Recommendations 2, 3
3. A formal, ongoing process through which the University can examine and, where necessary, address through policy vehicles the technical and societal changes that have an impact on University policy and practice in the areas of privacy and information security.	All recommendations

Defining Privacy

It is important to distinguish the intertwined concepts of *autonomy privacy* and *information privacy* from one another.

Privacy is about the individual. In the context of this report, it is also about the agreement ("terms and conditions") between the University and the individual that defines how privacy of that individual is handled.

Privacy comprises:

- **Autonomy privacy**: an individual's ability to conduct activities without concern of or actual observation; and
- **Information privacy**: the appropriate protection, use, and dissemination of information about individuals.

Autonomy privacy is an underpinning of academic freedom and is related to concepts such as the First Amendment's freedom of association, anonymity, and the monitoring of behavior; for example, by identifying with whom an individual corresponds or by building a profile of an individual through data mining. Autonomy privacy also encompasses records created by the individual such as research data, working drafts of research findings, communications of ideas, and opinions. It goes beyond the scope of (electronic) information and into the physical world when we speak of direct observation of individuals.

Information privacy is about an individual's interest in controlling or significantly influencing the handling of information about him or herself, whether it is an academic, medical, financial, or other record.

These concepts are not as clear and independent as their definitions may suggest.

Observations

The University's long experience with privacy, when viewed through the lens of the above definitions, reveals gaps, silos, and challenges in its approach to addressing privacy.

A survey of privacy models identified those that spoke only to information privacy or, even more narrowly, to compliance with statutory or regulatory requirements—the traditional realm of the privacy officer—and not to autonomy privacy. This proposal is intended to provide an integrated policy framework.

Another challenge is to promote convergence of the expectations of individuals with those of the University, which operates amid myriad legal and regulatory requirements, management demands, and operational issues. An individual, for example, may be willing to accept loss of personal information on a smartphone, whereas that phone may also contain information that the University is obligated to protect. These expectations are not easily reconciled under the University's existing policies. Individuals' expectations are based on different assumptions and constraints than are University policies.

Technology, social norms, and policy evolve at differential rates.

II. RECOMMENDATIONS

RECOMMENDATION 1: UW-Madison Statement of Privacy Values, UW-Madison Privacy Principles, and Privacy Balancing Process. The University shall formally adopt the proposed UW-Madison Statement of Privacy Values, Privacy Principles, and Privacy Balancing Process.

1. UW-Madison Statement of Privacy Values

The University of Wisconsin-Madison respects the privacy of individuals. Privacy plays an important role in human dignity and is necessary for an ethical and respectful workplace. The right to privacy is declared in the Wisconsin Constitution.

Privacy consists of (1) an individual's ability to conduct activities without concern of or actual observation, and (2) the appropriate protection, use, and release of information about individuals.

The University must balance its respect for both types of privacy with its other values and with legal, policy, and administrative obligations.

Academic and intellectual freedoms are values of the academy that help further the mission of the University. These freedoms are most vibrant where individuals have autonomy: where inquiry is free because it is given adequate space for experimentation and the ability to speak and participate in discourse within the academy is possible without intimidation.

Transparency and accountability are values that form the cornerstone of public trust. Access to information concerning the conduct of business in a public university and an individual's access to information concerning him/herself is a right of every citizen as stated in the Wisconsin Constitution.

Thus, the University continually strives for an appropriate balance between:

- ensuring an appropriate level of privacy through its policies and practices, even as interpretations of privacy change over time;
- nurturing an environment of openness and creativity for teaching and research;

- being an attractive place to work;
- honoring its obligation as a public institution to remain transparent, accountable, and operationally effective and efficient; and
- safeguarding information about individuals and assets for which it is a steward.

2. UW-Madison Privacy Principles

Autonomy Privacy Principles

Members of the University community are expected to uphold autonomy privacy, which is the ability of an individual to exercise a substantial degree of control over one's expressions, associations, and general conduct without unreasonable oversight, interference, or negative consequences. In the University setting, autonomy privacy is closely associated with the concepts of academic freedom, free speech, and community. The following proposed autonomy principles are intended to capture our culture of openness, transparency, ethical behavior, and respect for others:

Free inquiry

The University is guided by First Amendment principles and is committed to encouraging its members to exercise free discourse without fear of reprisal or intimidation, subject to the privacy and safety of other individuals or University resources.

Respect for individual privacy

The University is committed to respecting the privacy of individuals, including their interactions with others, and expects University members to esteem each other's privacy and well-being.

Surveillance

The University is guided by Fourth Amendment principles regarding surveillance of persons or places, whether in person on campus or electronically, and is committed to balancing the need for the safety of individuals and property with the individuals' reasonable expectation of privacy in a particular location.

Information Privacy Principles

The University is committed to providing individuals with a reasonable degree of control over the collection, use, and disclosure of information about themselves. The following principles provide guidance to the University for incorporating information privacy into its policies and practices:

Privacy by design

The University is committed to building privacy protections that embody the additional principles stated below into its business processes and information systems associated with the collection, use, and disclosure of information about individuals and about confidential information for which individuals are responsible. Business processes and information systems initiatives, revisions, or upgrades will be evaluated for consistency with the UW-Madison Privacy Principles and compliance with associated policies.

Transparency and notice

The University demonstrates its commitment to transparency by giving individuals reasonable advance notice of its information policies and practices for collecting, using, disclosing, retaining, and disposing of information about individuals.

The University expects its members to collect, use, disclose, and retain only the minimum amount of information about individuals as necessary for the specified purpose and to appropriately dispose of such information in accordance with the University's records-retention schedules.

The University expects its members who collect information about individuals to publish privacy notices that clearly inform individuals about the purposes (how information will be used or disclosed as permitted or required by law) and the scope of information collected.

Choice

Prior to collecting, using, disclosing, or retaining information about individuals, the University expects its members to provide individuals, whenever possible, with the ability to choose whether to and by what means to provide their information.

However, when the information about the individual is necessary to deliver a service or benefit or to participate in an activity, the individual may be required to provide the information in order to receive the service or benefit or to participate.

Information review and correction

Unless prohibited by law, the University is committed to providing individuals with a way to review the information about themselves that they have provided or permitted to be collected, as well as a procedure to request the correction of inaccuracies and one to perform the correction if appropriate.

Information protection

The University demonstrates its commitment to protecting information about individuals under its stewardship by providing appropriate employee training and by implementing privacy and information security controls.

Accountability

The University expects every individual to be aware of and accountable for complying with these principles and actively supporting the University's commitment to respect the privacy of individuals.

The University demonstrates its commitment to these principles by investigating reported violations of information privacy principles and policies and, as appropriate, taking corrective measures.

3. Privacy Balancing Process

The Privacy Balancing Process is intended as a tool to guide policy-making and decision-making when competing privacy interests, University values, or obligations exist and for which no statutory provision, common law, or University policy is directly applicable. The balancing process is derived from the UW-Madison Privacy Statement, applies the UW-Madison Privacy Principles, and rests on the acknowledgement that protecting autonomy privacy depends both on protecting information privacy and on ensuring information security.

The balancing process is intended to achieve consistency in privacy-related decisions. The process will be employed by governance bodies (described subsequently) in such a way that a cumulative body of institutional knowledge will inform policy development and routine practices of campus privacy officials and other UW-Madison managers. The process is applicable both to information that the University maintains about individuals (information privacy); as well as to their speech and behavior that is conducted on University premises, that uses University resources, or that is made in their role as a University representative (autonomy privacy).

A balancing decision depends on the specifics of each case, weighing multiple interests and impacts. The relative weights of many factors are analyzed to determine whether the proposed course of action is sufficiently compelling to justify the impacts. For example, proposals to monitor or to collect information about the activities of individuals must articulate a significant University or individual need for such activity. Such a "significant interest" stance gives reasonable deference to the privacy of individuals without unduly constraining institutional operational needs.

The balancing process analysis may result in a conclusion that one party's interest or position carries the most weight. For example, a University's policy to require individuals to identify themselves before entering certain campus buildings is approved because the University's obligation to protect the physical safety of individuals on campus outweighs an individual's privacy interest in anonymity. The balancing process could also result in striking a balance between the different interests, finding an acceptable middle ground that gives deference to each interest. The balancing process allows the University to remain flexible in light of changes in laws, societal norms, technological change, individual expectations, and University needs.

Privacy Balancing Analysis Factors

The balancing process must expressly consider the parties' interests, benefits, burdens, and consequences associated with the proposed action. Each analysis will differ depending on the action and the interests involved. A "party" in such an analysis may be, or represent, an individual, a community, or the University; with the recognition that parties may overlap or that a party may have multiple roles.

Some potential factors that are helpful to privacy analysis are given below. This list is not intended to be prescriptive; it is intended to illustrate how a balancing analysis would be conducted.

- What are the benefits to each party in successfully asserting privacy interests or a specific policy stance? What are the burdens, impacts, and risk to each party if the proposed action is not taken?

- What alternative approaches, or reasonable privacy protections, might be used in conjunction with the proposed action to make it less intrusive?
- What are the costs, whether in dollars, time, effectiveness, or other metrics?
- What actions have been taken (or could be taken) by each party to protect their own interests?
- What new technologies or processes might mitigate the privacy concerns, now or in the foreseeable future?

Campus Privacy (and Information Security) Board

RECOMMENDATION 2: Campus Privacy (and Information Security) Board. The Chancellor and Provost shall form a University Board to advise them, or a designee, on privacy and information security; set strategic direction for autonomy privacy, information privacy, and information security; champion the UM-Madison Privacy Values, Principles, and Balancing Process; and monitor compliance and assess risk and effectiveness of campus privacy and information security programs.

Campus Board Responsibilities:

Setting strategic direction

- Setting strategic direction in the areas of privacy and information security for the campus; considering issues in these areas and their impact on the campus and the communities it serves
- Staying current on new developments in privacy and information security, including related technology developments
- Recommending issues for system-wide consideration as appropriate

Risk, compliance, and effectiveness

- Application of the privacy balancing process to resolve competing interests
- Assembling, reviewing, and approving the sharing of balancing analyses among campuses
- Ensuring that the campus privacy program delivers fair and consistent decisions
- Ensuring that the campus privacy and information security programs have sufficient visibility and executive support
- Monitoring campus compliance with UW-Madison Privacy Values and Principles
- Assessing the effectiveness of the campus privacy and information security programs
- Reporting annually for transparency

Campus Privacy Official

RECOMMENDATION 3: Campus Privacy Official. The Chancellor and Provost shall designate a privacy official to be responsible for the collaborative development, implementation, and administration of a unified privacy program for the campus. The privacy official shall work closely with the campus's privacy and information security board.

A successful campus privacy program requires knowledgeable privacy leadership and an engaged campus community. The privacy official should be at a level able to effect organizational change within the University context of shared governance, mission, and values; and complex information technology infrastructure and operations.

The privacy official shall work closely with the campus's privacy and information security board on the vision, strategies, and methodologies of the campus privacy program; and collaborate with the campus's information security officer and other functional experts.

A campus privacy program encompasses viewpoints and expectations from the campus community and the legal and technological landscapes and addresses both autonomy and information privacy in:

- Identifying and managing privacy risks;
- Developing privacy policies and practices;
- Maintaining integrity over campus practices and decisions that impact privacy;
- Fostering privacy by design;
- Properly handling privacy breaches;
- Resolving conflicting privacy interests and ensuring the application of the balancing principles where appropriate; and
- Actively exploring technologies and methods that can help to protect privacy.

Infusing understanding and use of the UW-Madison privacy values and principles across the community in routine academic and administrative operations is fundamental to meeting the challenge of shifting expectations, new laws, and emerging technologies. A key responsibility of the campus privacy official will be addressing this need, whether in clarifying the boundaries of personal privacy, which is at the heart of the complex and vexing issue of the commingling of University information with personal information, or in promulgating the expectation that University privacy and information security principles extend to relationships with partners and collaborators.