PRIVACY NOTICE WORKSHOP

Dr. Whitney Phillips
State Privacy Officer
wphillips@Utah.gov

Nora Kurzova, JD.
Assistant State Privacy Officer
nora.kurzova@Utah.gov

OFFICE OF THE
STATE AUDITOR

Privacy Policies and Notices

What

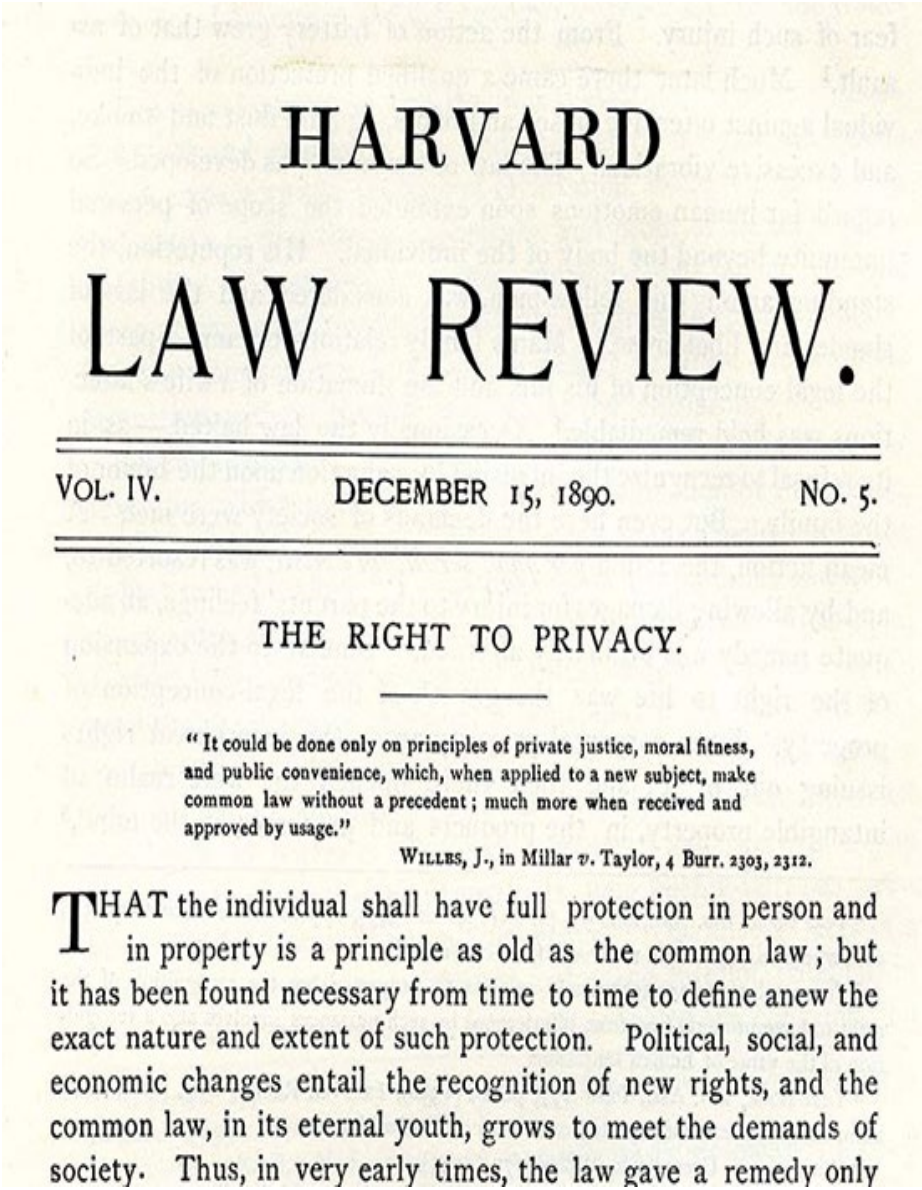
- A description of an organization's information management practices.

Why

- *Educate* users about how personal data is used.
- *Increase trust* between organization and individual.
- *Help* individuals assert control over how their personal data is used.
- *Accountability* of organization.
- *Legal protection* from claims that organization did not provide notice of personal data usage.

Privacy Defined

- A nebulous philosophical, legal, social and technological concept which means different things to different observers.
- Harvard Law Review article in 1890 by law partners Samuel Warren and Louis Brandeis.
- The article defined privacy as “a right to be let alone.”*
- Four main areas of privacy are of particular interest with regard to data protection and privacy laws and practices:
    1. information privacy
    2. bodily privacy
    3. territorial privacy, and
    4. communications privacy



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

* Judge Thomas Cooley first used this phrase in *A Treatise on the Law of Torts 29 (2d ed.* 1888) – referred to right to be free from physical attack and injury.

Source: IAPP Glossary

https://iapp.org/resources/glossary/

Privacy and the US Constitution

- The Constitution does not contain an explicit right to privacy.
- This “right” comes from common law and is inferred from various constitutional amendments.

Constitutional Amendments and Privacy

- 1st: freedom of speech and assembly
- 3rd: zone of privacy of home
- 4th: no unreasonable searches and seizures
- 5th: no self-incrimination.
- 9th: protection of rights not provided for in the first eight amendments.
- 14th: no infringement without due process

Olmstead vs US - 1928
US Supreme Court

- bootlegging
- illegal wiretap
- defendants say wiretap violated 4th and 5th amendment
- Court upheld conviction 5-4
- Court said 4th amendment only applied to physical search and seizure
- ruling overturned in 1967

- Dissent - more famous than the outcome and influenced later Court decisions about privacy expectations

Justice Louis Brandeis dissent

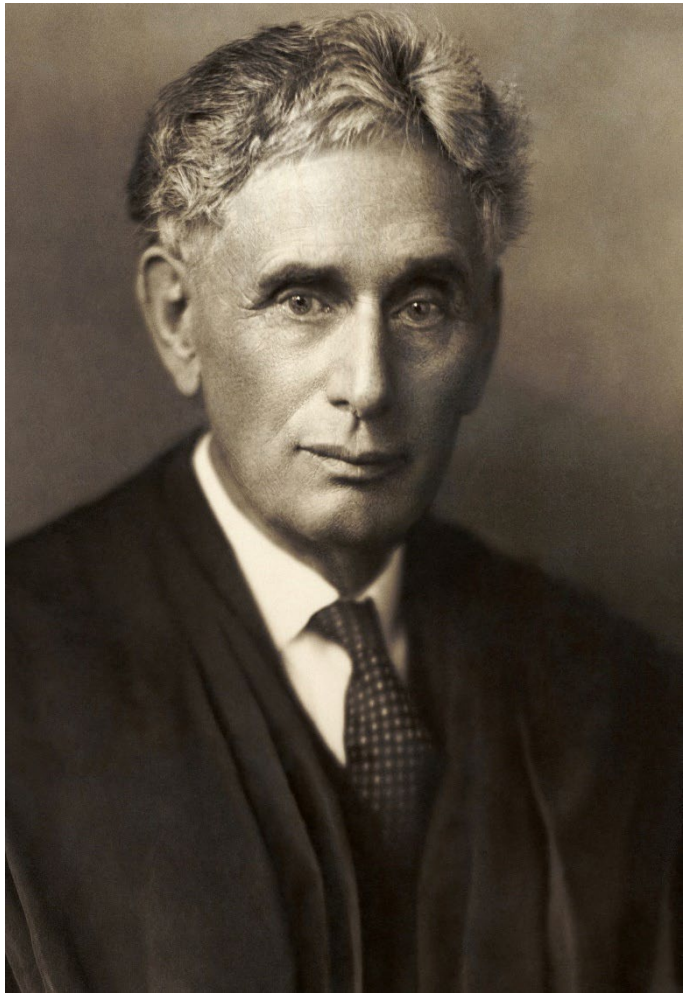
"The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness.

They recognized the significance of man's spiritual nature, of his feelings, and of his intellect.

They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things.

They sought to ***protect Americans*** in their beliefs, their thoughts, their emotions and their sensations.

They conferred, as against the Government, ***the right to be let alone**** – the most comprehensive of rights, and the right most valued by men."



Privacy Policy vs Privacy Notice

Policy

- **Internal** statement
- directed at handlers and decision makers
- how an organization handles personal information
- instructs on collection, use, storage and destruction of data, and data subjects rights
- may referred to as a data protection policy

Notice

- **External** statement
- made to a data subject
- describes how an organization collects, uses, retains and discloses personal information
- may be referred to as a privacy statement, fair processing statement, privacy policy

Federal Law

The US does not have a comprehensive federal privacy law.

Rather, various federal regulations govern privacy policies for specific circumstances.

- HIPAA - healthcare
- Graham-Leach-Bliley Act – financial sector
- COPPA - Children's Online Privacy Protection Act
- Fair Credit Reporting Act – credit reporting agencies
- Privacy Act of 1974 – need for info vs. individual rights against unwarranted invasion of privacy

State Law: Governmental Internet Information Privacy Act (63D-2-103)

63D-2-103. Collection of personally identifiable information.

(1) A governmental entity **may not collect** personally identifiable information related to a user of the governmental entity's governmental website unless the governmental entity has taken reasonable steps to ensure that on the day on which the personally identifiable information is collected the governmental entity's governmental website **complies with Subsection (2).**

"Governmental entity" means:

a. an executive branch agency as defined in Section 63A-16-102;

b. the legislative branch;

c. the judicial branch;

d. the State Board of Education;

e. the Utah Board of Higher Education;

f. an institution of higher education; and

g. a political subdivision of the state:

i. as defined in Section 17B-1-102; and

ii. including a school district.

"Personally identifiable information" (PII) means information that identifies:

a. **a user by:**

i. name;

ii. account number;
iii. physical address;
iv. email address;

v. telephone number;

vi. Social Security number;

vii. credit card information; or
viii. bank account information;

b. **a user** as **having requested or obtained** specific materials or services from a governmental website;

c. Internet sites **visited by a user**; or

d. any of the **contents** of a **user's data-storage device**.

Subsection (2)

63D-2-103. Collection of personally identifiable information.

(2) A **governmental website *shall* contain a privacy policy statement** that discloses:

(a)

(i) the **identity** of the governmental website operator; and

(ii) how the governmental website operator may be **contacted**:

(A) by telephone; or

(B) electronically;

(b) the personally identifiable **information collected** by the governmental entity;

(c) a **summary** of how the personally identifiable information is used by:

(i) the governmental entity; or

(ii) the governmental website operator;

(d) the **practices** of the following related to disclosure of personally identifiable information collected:

(i) the governmental entity; or

(ii) the governmental website operator;

(e) the **procedures**, if any, by which a user of a governmental entity may request:

(i) access to the user's personally identifiable information; and

(ii) access to correct the user's personally identifiable information; and

(f) without compromising the integrity of the security measures, a general description of the **security measures** in place to protect a user's personally identifiable information from unintended disclosure.

“Privacy Policy” Statement

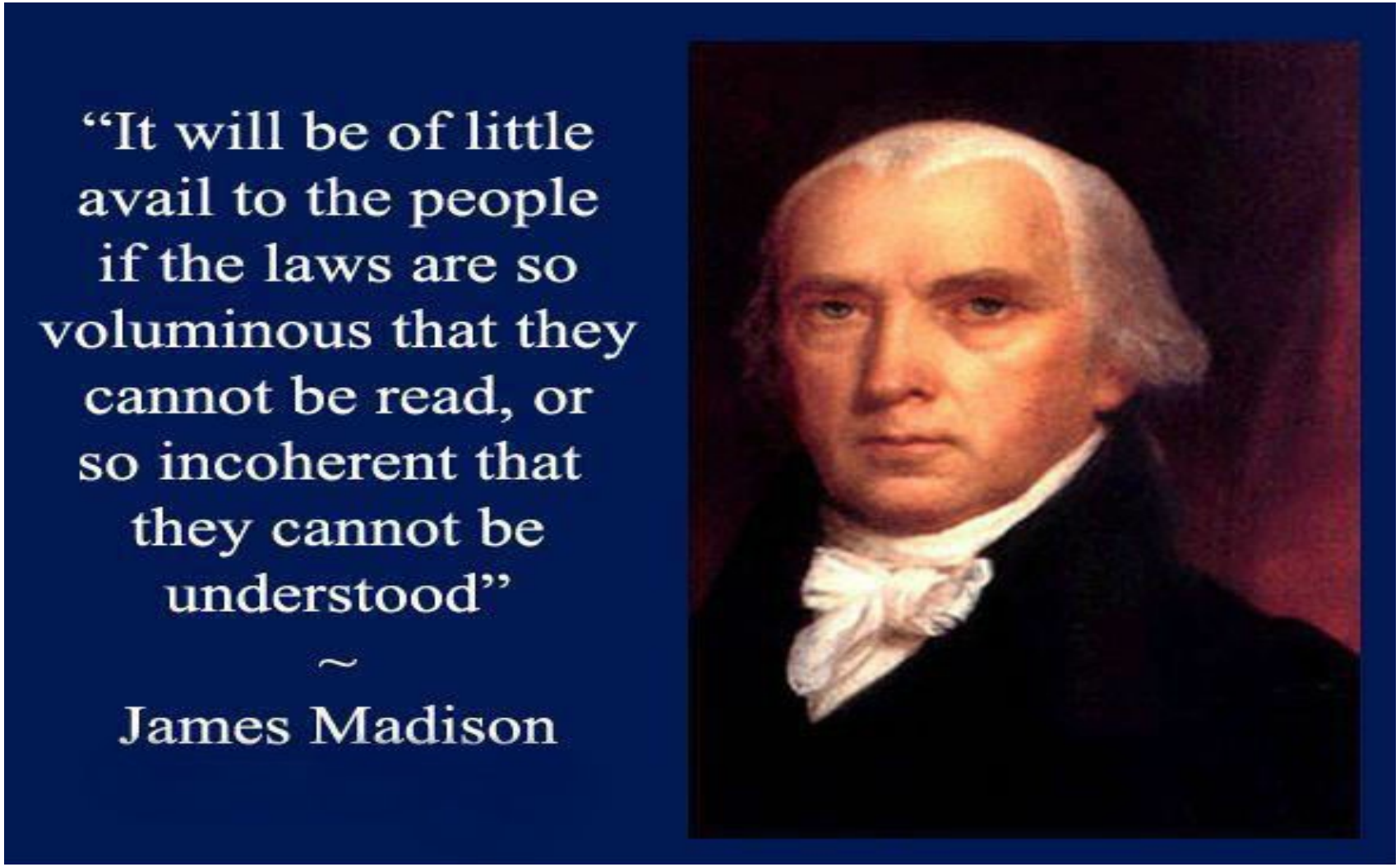
1. Identity and contact information of the website operator
2. PII Collected
3. Summary of how the PII is used by government entity or website operator
4. Practices related to disclosure of PII by government entity or website operator
5. Procedures (if any) of how a user may request access and/or correct the user’s PII
6. Security measures to protect from unintended disclosure

Choice

- A person's ability to **specify whether their personal information will be collected and how it will be used** or disclosed.
- A person's consent can be expressed or implied
  - With ***express consent*** (also called affirmative consent), a person actively gives concern, or "opts in," to the collection and use of their data
  - With ***implied consent***, a consent is assumed unless a person actively "opts out" by withdrawing their consent

Drafting the Notice

keep it simple

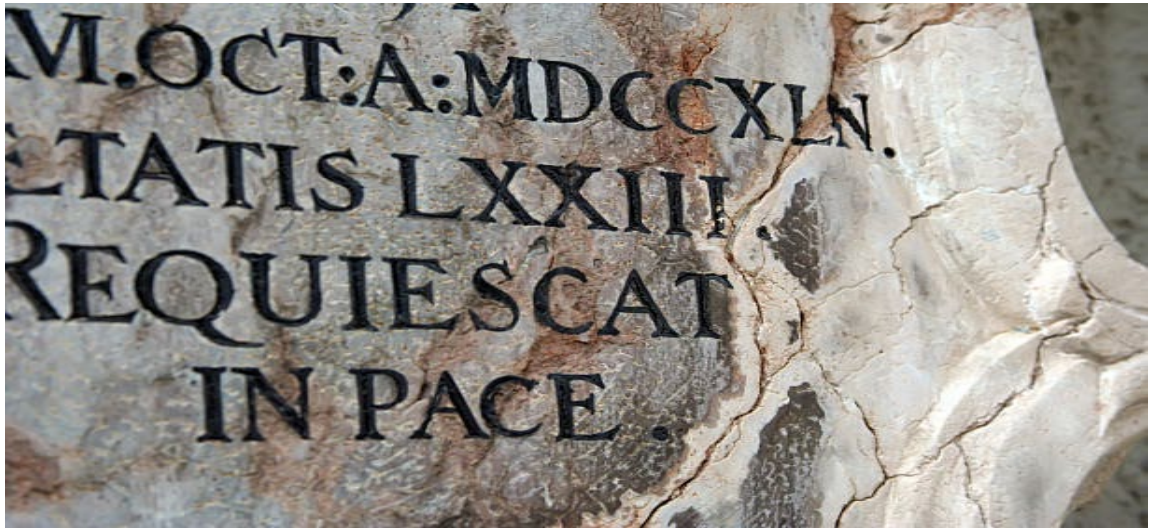


Additional Considerations

1. Name of organization (don’t overlook the obvious)
2. Effective date or last update
3. Lawful basis for PII collection
4. Rationale of why PII is collected
5. With whom and how PII is shared or NOT shared
6. How long PII is stored
7. Under what circumstances PII cannot be removed (GRAMA)
8. Resources for learning more about privacy rights (links)
9. Where a user can file a complaint regarding their privacy

User Experience Recommendations

1. Transparent
   - Accurate
   - Easy to find
2. Accessibly written
   - Easy to understand
   - Avoids legal jargon
3. Layered Approach
   - Gives users options
   - Avoids TLDR (too long, didn't read)
   - Puts essential information out front.
   - Provides information that is helpful, but not required.



Collaboration Partners Recommendations

- Cyber security
- Information technology
- Legal
- Human Resources
- Communications
- Public Relations
- Records Officer
- Administration
- Public Utilities
- Third-party vendors

Let’s Review your Privacy Policy Statement

Volunteers?

https://ww.sgcity.org/privacypolicy/