0036

2005 General

State of Utah

Department of Natural Resources

MICHAEL R. STYLER
Executive Director

Division of Oil, Gas & Mining

JOHN R. BAZA
Division Director

JON M. HUNTSMAN, JR.
Governor

GARY R. HERBERT
Lieutenant Governor

August 9, 2005

TO: Coal Program file

FROM: Mary Ann Wright, Associate Director, Mining

SUBJECT: Requirements of for OGM imposed by Governmental Internet Information Privacy Act, (GIIPA)

The Natural Resources Division of the Attorney General's Office has researched, at OGM's request, whether OGM is required to have its own Privacy Policy under GIIPA. The concern centers on information in our PIC room and information available in scanned documents that will soon be made available over the web via the implementation of our electronic permitting process. A number of these public documents contain personally identifiable information, as defined by GIIPA. The question was asked: "Does OGM need to write a Division Policy Statement to comply with the state regulatory requirements of GIIPA?" The AG's office responded that when merely making information available on the Internet that is already properly classified under GRAMA, that information would retain the same protections when it is made available over the Internet.

However, when or if OGM reaches a point of collecting personal data online (for a permit application) then a policy will be needed. At that point, OGM may choose to either incorporate the state's existing privacy policy, or prepare an OGM-specific policy not inconsistent with the state-wide policy.

For further background discussion, please refer to the attached Memorandum on this issue, dated June 30, 2005.

Attachments
cc: Mary Ann Wright
Pam Grubaugh-Littig
D. Wayne Hedberg
Randy Harden
P:\GROUPS\MINES\WP\AMAW\Memo privacy internet policy.doc

1594 West North Temple, Suite 1210, PO Box 145801, Salt Lake City, UT 84114-5801
telephone (801) 538-5340 • facsimile (801) 359-3940 • TTY (801) 538-7458 • *www.ogm.utah.gov*

MEMORANDUM

TO: Alison Garner, Assistant Attorney General, Natural Resources Division

FROM: Jim Allen, Law Clerk, Natural Resources Division

RE: Privacy Policy Requirements Imposed on Department of Oil, Gas, and Mining Public Information Website by the Governmental Internet Information Privacy Act of 2004

DATE: June 30, 2005

ISSUE

Under the Governmental Internet Information Privacy Act of 2004, must the Division of Oil, Gas, and Mining publish and implement a privacy policy when it makes its public records available on the Internet?

BRIEF ANSWER

No. The Governmental Internet Information Privacy Act (GIIPA) imposes no new requirements on the Division's website, so long as that website merely provides access to existing state records and does not collect information. GIIPA applies only to collection of personally-identifiable information from visitors to and users of state and local government websites, and specifically provides that access to government records remains under the control of the Government Records Access and Management Act (GRAMA). However, the website may not ask visitors to supply information, nor employ any background processes that collect personally-identifiable information from site visitors unless it also provides a privacy policy that complies with the requirements of GIIPA.

ASSUMPTIONS

1. For purposes of this memo, I assume that any information placed in DOGM's physical Public Information Center has been properly classified ~~as public~~ under GRAMA.

2. I also assume that DOGM has complied with any federal or state statutes regarding access to records that are specific to DOGM or the programs they administer.

DISCUSSION

ISSUE 1: UNDER THE GOVERNMENTAL INTERNET INFORMATION PRIVACY ACT OF 2004, MUST THE DIVISION OF OIL, GAS, AND MINING PUBLISH AND IMPLEMENT A PRIVACY POLICY WHEN IT MAKES ITS PUBLIC RECORDS AVAILABLE ON THE INTERNET?

No new privacy policy is required by GIIPA when the Division makes its previously available public records available on the Internet through its website. GIIPA prohibits an agency of state government from collecting personal information from users of websites unless the agency has a policy governing the information's use, and advises site visitors of the policy. Utah Code Ann. § 63D-2-103(1) (2005). Collecting information, for the Act's purposes, means gathering data from or about a user of a government website. § 102(1)(a). GIIPA specifically provides that access to government records remains under the control of GRAMA, and that nothing in GIIPA shall affect the classification of records as private, protected, controlled, or limited under GRAMA. § 103(3)(a)-(b).

While GRAMA concerns itself with how and when the public shall have access to government records that may or may not contain personal information, GIIPA is concerned with the prospect that personal information may become part of a potential government record without the owner's consent, or even knowledge. *See generally* Utah Attorney General's Office, *Handbook for the Utah Government Records and Management Act* 2 (2005). As government entities expand their use of the internet to provide information and conduct business, GIIPA

assures that no new information will be obtained as a byproduct of a member of the public's use of the government's internet website.

Rules promulgated by the state's chief information officer (CIO) prior to GIIPA provide that state agencies operating websites may either incorporate the state privacy policy or prepare one of their own not inconsistent with the state's. Utah Admin. Code R365-5-5 (2005). Such a policy may only be less protective of personal information if another federal or state law mandates it, and the agency must inform the public of that mandate by posting its own agency-specific privacy policy. *Id.* As with GIIPA, the CIO's rules apply only to personally identifiable information that is obtained by the state agency through the operation of its website. R365-5-1(1). The rule identifies personal information as name, physical address, e-mail address, telephone number social security number, credit card and bank account information, and any combination of personal information that could be used to determine identity. R365-5-4(a)-(h). The rule applies to "individuals" which I take to mean natural persons (real people) as distinct from businesses and organizations. R365-5-4(4).

Under the rules, an agency that is contemplating an online "application" (in the software sense, roughly synonymous with "program") must complete a "privacy risk assessment" prior to the time the application is placed online and made available to the public. R365-5-4(9), 7(3), 8. Again, this assessment pertains only to the information that might be collected online, and not to the content of records in the online application. R365-5-4(4), 6(1). GIIPA extends the scope of the CIO's rule in two ways: first, it extends applicability to certain agencies exempted by name from the CIO's rule, to the judicial and legislative branches, and to political subdivisions of state government, Utah Code Ann. § 63D-2-102(3)(b)-(g), and; second, it adds information commonly gathered by some web applications' background processes (such as cookies, robots, and

spyware) to the list of personal information that may not be collected unless GIIPA's notice provisions are observed. § 63D-2-102(6)(b), (c), (d).

There are two circumstances that might arise in the course of putting the PIC records online that would invoke GIIPA and the CIO rules. First, the website may not ask a site user or visitor to supply any personal information. If the site requires a user ID and password, those should be either randomly assigned, or chosen by the user under advice not to use a personally identifiable ID. Second, the software may not collect identifiable information, such as e-mail addresses, Internet protocol (IP) addresses, machine names, uniform resource locators (URLs), or any other information that came from the visitor's computer, if that information might serve to identify a person. GIIPA also prohibits collecting data that connects a person's identity with the information they view or request, or the Internet sites they visit. If it is necessary to do any of these things, then a policy must be adopted that advises sites users of the information collected and how it will be used. A future modification of the site to allow DOGM customers to transact business with the Division would trigger the requirements of GIIPA and the CIO rules.